Juridiska institutionen

Examensarbete vårterminen 2014
Juristprogrammet
30 högskolepoäng

Transacting Trade Secrets

Enabling Commercial Transactions of Trade Secrets Utilising Law, Contracts, and Practical Measures

Denis Ilecic & Gustav Svensson

Handledare: Leif Östling
Examinator: Kristoffer Schollin

GÖTEBORGS UNIVERSITET
HANDELSHÖGSKOLAN

Abstract

Trade secrets represent great value in companies and grants competitive advantages. However, they are mainly used internally as a complement to IPRs in order to protect the knowledge of the company. This thesis investigates the possibility to generate value from trade secret by external use, i.e. transacting the trade secret through either selling or licensing. In order to visualise the findings the thesis is built around two different types of cases, one case where the knowledge is embedded inside a physical product and one where the knowledge is openly available in a manual, to give more comprehensive conclusions. Three different types of protection and control mechanisms are analysed, namely Swedish and EU trade secret legislation, contractual protection, and practical protective measures. It is found that each type of protection and control mechanisms does not grant a sufficient level of protection and control by itself. However, by combining the findings from the three parts the conclusion is arrived to that the protection and control should most times be sufficient for externally transacting trade secrets.

Acknowledgements

We would like to begin with thanking Martin Jansson, Manager Intellectual Assets Group IA & IP at SKF, for providing us with the opportunity to write this thesis at SKF and for being supportive and helpful throughout the work. Furthermore we would like to thank Bowman Heiden and Leif Östling for their support, insights, and for helping us with setting the course.

Denis Ilecic & Gustav Svensson

Gothenburg, Sweden May 2014

Table of Contents

Table of Figures

List of Abbreviations

ECU - Engine Control Unit
FHL - Act on the Protection of Trade Secrets (1990:409)
IP - Intellectual Property
IPR - Intellectual Property Right
KBC - Knowledge-based Capital
KBE - Knowledge-based Economy
NDA - Non-Disclosure Agreement
NDT - Non-Destructive Testing
OEM - Original Equipment Manufacturer
R&D - Research & Development
RAM - Random Access Memory
SME - Small & Medium Enterprises
SOU - Statens Offentliga Utredningar
USD - United States Dollar
WIPO - World Intellectual Property Organisation

List of Translations

English	Swedish
Trader	Näringsidkare
Economic Activity	Näringsverksamhet
Government Bill	Proposition
Title deeds	Lagfart
Official trustee	Konkursförvaltare
Engine Control Unit	Styrbox
Bankruptcy Estate	Konkursbo
Preparatory Works	Förarbeten
Right to Litigate	Talerätt
Exclusion Clause	Friskrivningsklausul
Contracts Act (1915:218)	Avtalslagen (1915:218)
Act on Protection of Trade Secrets (1990:409)	Lag om skydd för företagshemligheter (1990:409)

1 Introduction

It is well established that patents, copyrights, design rights, and trademarks can be transacted, either by sale or license. Companies have developed business models surrounding licensing of their patented technology as one of their main income source. Artists and record labels license out their copyrights on a daily basis, using for example Spotify as a mean. Companies utilising sub-contractors for production of their goods, such as Nike, are depending on licensing out their design rights to do business. Trademarks are licensed when a subcontractor is brewing and selling beverages under another brewer's trademark, such as when Coca Cola is brewed and sold by a local brewery in Sweden. These IPRs are traditional ways of protecting knowledge in order it to be transacted. However, not all knowledge is possible to protect by IPRs. For example inventions might lack the inventive step. There might also be business reasons for not utilising IPRs. These problems are to some extent offset by protecting of knowledge as trade secrets. Trade secrets are, due to their nature, not as commonly transacted as IPRs. The reason for this is due to the high risks of losing control and thereby the value of the trade secret. To investigate the level of protection and to understand the risks and how they can be avoided, a thorough analysis of Swedish and EU trade secret legislation will be performed.

Trade secrets represent great values in companies and society. It is therefore unfortunate that trade secrets are not given more protection in countries within the EU. For instance Sweden is the only state in the EU with an explicit act on protection of trade secrets. As an attempt to address this, the European Commission has proposed a Directive for harmonizing the trade secret protection throughout the European Union.

This thesis is a cooperation with SKF, who presented the authors with the subject and a wish for investigate and analyse how to transact trade secrets while maintaining their characteristics as trade secrets. The thesis will therefore be focused on the situation of SKF, but general conclusions will also be drawn.

1.1 Problem Statement

When performing the literature review for this thesis the problems presented in the following have been identified.

1.1.1 Volatile Nature of Knowledge and Trade Secrets

The first problem is that of the characteristics of knowledge, intangibles, compared to physical goods, tangibles. This poses problems in, for example, situations of bankruptcy where, for tangibles,

it is fairly easy to decide ownership compared to deciding ownership of intangibles not protected by IPRs. Furthermore it is identified that transacting tangibles present less obstacles than transacting intangibles, due to the volatility of intangibles.

1.1.2 Lack of Exclusivity

While "knowledge is the currency of the new economy", as the EU-commission puts it, this knowledge can be protected by several means.[1] The most well known ways of doing this is by using IPRs. These IPRs grant the owner exclusive rights to what is claimed by the IPR. However, this is not the case when one chooses, for one reason or another, to protect her proprietary knowledge as a trade secret. As there is no exclusivity right for trade secrets, this implies that once the information is out in the open anyone can freely use it. This volatile nature makes it difficult to transact trade secrets, in for instance licensing agreements, as it will be difficult to govern these agreements and ensure that the trade secrets do not lose their status as trade secrets and thereby their value.

1.1.3 Differences in Protection

The lack of harmonized legislation adds to the hardship of transacting trade secrets. If a company does not know what kind of protection its trade secrets has in each country, the company is certainly less prone to transact its trade secrets. With the Directive the legislation for trade secrets might be harmonised within the EU. If the Directive is adopted the problem will not be whether the protection is sufficient in a certain country, but rather how to transact the trade secret in order to generate the most value with the Directive in force.

1.1.4 Static Legislation

As is presented in the theory section below, IP may be used either statically or dynamically, where using IP in transactions such as licensing is a typical example of dynamic use. However, the trade secret legislation in Sweden, as well as the Directive, is not designed with dynamic use in mind. The legislation is instead designed for static use, i.e. keeping the trade secret hidden and granting certain measures if the trade secret is misappropriated.

1.2 Aim of The Thesis

The aim of this thesis is to investigate how the concept of knowledge, as an asset and property, can be treated as dynamic property in a commercial transaction by setting up foundations for a platform

[1] European Commission (July 2012a), Communication from the Commission to the Europeans Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Reinforced European Research Area Partnership for Excellence and Growth,COM(2012) 392, 17.7.2012, p. 2.

consisting of protective measures. Three different types of protective measures will be analysed, namely Swedish and EU trade secret legislation, contractual provisions, and practical measures. Emphasis will be on trade secret legislation since this is the foundation of the thesis. Each of the three types of protection will henceforth be referred to as 'blocks'. The thesis will build upon two scenarios, which are inspired from two real cases from SKF where the authors will be responsible for one case each. In the first case the trade secret, and the knowledge it comprises, is embedded within a physical product and therefore not openly available for the customer. In the second case the trade secret, and the knowledge it comprises, is openly available for the customer. In relation to each case the most imminent risks associated with transacting trade secrets will be analysed. Using two cases in conjunction with their respective imminent risks, the authors' believe will enable more concrete insights. If not using two examples there is a high risk that the thesis will have a more speculative character and less focused.

1.3 Research Questions

In order to break down the broad scope the thesis will focus on three research questions, with sub-questions, that will be applied to both cases individually. The following research questions are investigated:

1. Can the knowledge be identified as a trade secret according to the legal definition of the FHL and the Directive?
    1. What protection is granted by the FHL and the Directive in order to protect the knowledge from the imminent risks?
    2. Does the protection granted by the FHL and the Directive suffice for the knowledge to be treated as dynamic property in a commercial transaction?
2. What contractual provisions can be utilised in order to protect the knowledge from the imminent risks?
    1. Does the protection granted by contractual obligations suffice for the knowledge to be treated as dynamic property in a commercial transaction?
3. What practical measures can be used in order to protect the knowledge from the imminent risks?
    1. Does this protection granted by the practical measures suffice for the knowledge to be treated as dynamic property in a commercial transaction?

2 Literature Review

Trade secrets and their use have been addressed in several works. In "Immaterialrätt & sakrätt" Wainikka addresses the question whether or not trade secrets can be licensed, however, she does this very shortly by just stating that it is possible and without mentioning how it should be done.[2] Wainikka has further addressed, to some extent, the use of trade secrets to protect innovations in the work "Att skydda innovationer", however, trade secrets are only a minor part in the work and focus is not on transacting trade secrets but rather she gives a short account for how to protect trade secrets internally.[3] Helgesson has performed a thorough comparative analysis of trade secret protection in France, Germany, Netherlands and Sweden, in order to show the connection between technical development, socio-economical factors and the law, where the goal is to see how trade secrets may work in a new technical reality.[4] Tonell thoroughly analyses the use of NDAs and their relation to trade secrets in his work "Sekretessavtal - och det rättsliga skyddet för företagshemligheter."[5] This work addresses to some extent the external transfer of trade secrets, mainly in connection to NDAs, however, focus is on internal use of trade secrets in order to protect knowledge. Fahlbeck presents a thorough analysis of the FHL in his work "Lagen om skydd för företagshemligheter – en kommentar och rättsöversikter" with the focus on explaining the law, preparatory works, and relevant case law.[6] Focus is to explain how the law is to be understood rather than how to facilitate external use of trade secrets. Previous master theses regarding trade secrets have been addressed to some extent. Winkler's thesis "Secrecy as a Part of the Intellectual Value Creation Within a Firm" focuses on how secrecy can be used to generate value within the company, and not through external uses.[7] Stenberg and Fransson addresses in their thesis "Företagshemligheter - en värdeskapande strategi" also how trade secrets can be used to generate value as well as questioning that the FHL is arranged under competition law in Sweden.[8] It is safe to say that how trade secrets should be handled internally in a company has been thoroughly researched. However, using trade secrets externally have been mentioned as possible in the

[2] Levin, Marianne, Wolk, Sanna, Persson, Annina H., Immaterialrätt & Sakrätt, Upplaga 1, Jure, Stockholm 2002.

[3] Wainikka, Christina, Att skydda innovationer: Affärer, risker och möjligheter, Upplaga 1:1 Studentlitteratur, Lund.

[4] Helgesson, Christina. Affärshemligheter i samtid och framtid, Upplaga 1:1, Jure, Stockholm 2000.

[5] Tonell, Magnus, Sekretessavtal - och det rättsliga skyddet för företagshemligheter, Upplaga 1, Jure, Stockholm 2012.

[6] Fahlbeck, Reinhold, Lagen om skydd för företagshemligheter - En kommentar och rättsöversikter, 3rd Edition, Norstedts Juridik, 2013.

[7] Winkler, Emil, Secrecy as a part of the intellectual value creation within a firm – How to use secrecy as a strategic tool in a business, University of Gothenburg – School of Business, Economics and Law, 2010.

[8] Stenberg, Susanne, Fransson, Martin, Företagshemligheter – En Värdeskapande Strategi, Juridiska Institutionen – Handelshögskolan vid Göteborgs Universitet, 2002.

encountered sources but have not been thoroughly researched in terms of how to do it.

3 Method and Material

The imminent risks of each case are a product of structured brainstorming, as well as discussions with relevant personnel at SKF and the supervisor.

3.1 First and Second Research Questions

For the first two research questions of the thesis, including both FHL and the Directive as well as the contractual provisions, the methodology that will be used is legal method. This method can be summarised in three steps:[9]

1. Find all relevant legal information - Laws, case law, legislative proposals, doctrine etc. that is relevant for the research question.
2. Apply the found legal information to the actual research question by interpreting them. This interpretation can be done in various ways, e.g. by literary interpretation, by teleological interpretation, according to the systematicity of the legislation in general, etc.
3. Argue for the case that the legal sources and the interpretation of them is the correct one.

The conclusion arrived to by using the legal method is then analysed in relation to the theories under the theory section. This is done by first reading up on the theories, then applying them to the conclusion where applicable and finally arguing for that the conclusion falls within the scope of the theories.

3.1.1 The Directive

As the Directive is not yet adopted by the EU, and therefore there is no existing case law, it is difficult to analyse what the prerequisites implies on a more detailed level. Due to this different interpretation methods utilised by the European Court of Justice will be reviewed as basis for analysing the Directive.

When the European Court of Justice handles a case they may use various different methods, such as literary interpretation, autonomous interpretation, comparative interpretation, teleological interpretation etc., as foundation for interpretation of the applicable rule.[10] The interpretation method the ECJ is most famous for is the teleological interpretation, which is mostly used when a

[9] Sandgren, Claes, Rättsvetenskap för uppsatsförfattare – Ämne, material, metod och argumentation, 2nd Edition, Norstedts Juridik 2007, pp. 36-39.

[10] Hettne, Otken Eriksson (2011), p. 158.

provision's wording or context is unclear.[11] A literary interpretation is mostly used in situations when the court want to use the wording of a provision as a limiting factor when, i.e. not wanting to give a provision a wider implication.[12] Hettne and Otken Eriksson states that since the EU law should have the same effect in all member countries one can assume that terms occurring in both national and EU-law should not be interpreted the same way.[13] A comparative method is according to Hettne and Otken Eriksson used for several reasons, such as to investigate if several countries have a similar solution to a problem, if there are differences in nations' regulations to use as argument for a decision, if a country has a design of a legal rule that could serve as a model for EU regulation and to ensure that the EU-law is not too far from the legal traditions of the member states.[14] Considering the influences taken from the FHL when drafting the Directive, together with the possibility to use national law when interpreting EU provisions, a comparison to how the Swedish act on trade secrets has been interpreted will be made in this thesis while having the implications of an autonomous and teleological interpretation in mind.

3.2 Third Research Question

Given that there is no source addressing the combination of trade secrets and practical protective measures, and that the nature of the question requires creativity, the method that will be used consists of structured brainstorm sessions, discussions that will be held with personnel at SKF working with IP and with a background in mechanical engineering, as well as interviewing an industry actor. In addition to this Internet searches for specialist knowledge, generally on technical forums, will be performed.

The conclusion arrived to by using the method above is then analysed in relation to the theories under the theory section. This is done by first reading up on the theories, and then applying them to the conclusion where applicable and finally arguing for that the conclusion falls within the scope of the theories.

3.3 Chosen Material

The chosen material can be divided between the three first research questions. Material in relation to the first research question can in turn be divided into two parts, one considering the Swedish legislation and one concerning the European legislation about trade secrets. For the Swedish

[11] Hettne, Otken Eriksson (2011), p. 159.
[12] ibid., p. 168.
[13] ibid., p. 161.
[14] ibid., p. 162 - 163.

legislation about trade secret the starting point is the propositionen 1987/88:155 that is the preparatory work of the FHL and has been consulted as far as it is applicable. Reinhold Fahlbeck's book "A comment on Act on the Protection of Trade Secrets" (authors' translation) is the most comprehensive work addressing the FHL and is the main doctrine for this thesis. Other doctrine will be used as well in order to confirm or to give a more nuanced view, however, in many cases the other sources derive their information from Fahlbeck's work or are not as comprehensive as Fahlbeck, why Fahlbeck is many times the only available source. These sources are the works of specialised lawyers within relevant fields of law. To understand the implications of the FHL in the judicial arena relevant case law will be studied when applicable.

For the European legislation on trade secrets the starting point is the Directive in itself. To understand the underlying considerations for the Directive the "Commission Staff Working Document Impact Assessment" will be consulted. This working document builds on the commissioned study conducted by Baker & McKenzie, which is a thorough investigation of the trade secret protection throughout Europe, USA, and Japan.[15] In order to understand the implications and how to interpret the Directive the work by Hettne and Otken Eriksson will be used.

The second research question regards many different areas of law. The starting point is contract law where the works of Ramberg and Ramberg is the main source. To understand the implications of contractual penalties the works of Gorton and Adlercreutz will be the main source. However, much of the before used doctrine are also relevant for the second research question, why they will be consulted here as well.

The nature of the third research question implies that no doctrine is available and few other sources as well. To understand and confirm the found solutions focus will be on Internet sources with specialist knowledge from technical forums to support and challenge the brainstormed theories used. The validity of the sources can, and should be, questioned. However, given the unorthodox nature of the solutions this is a necessity.

3.4 Flowchart

This thesis is written by two authors that need to be individually valued and judged, which has structural implications. In order to simplify for the reader the flowchart below has been made, see Figure 1.

[15] de Martinis, Lorenzo, Gaudino, Francesca, Respess, Thomas S. III, Baker McKenzie Study on Trade Secrets and Confidential Business Information in the Internal Market, Milan 04.2013.

The thesis is divided into three blocks, one for each of the three research questions. The first block answers the first research question whereas the second block answers the second research question and the third block the third research question. Using this structure makes the thesis more defined as well as it facilitates answering the research questions. It furthermore separates the findings making it more accessible for the reader.

The three blocks are in turn divided into two sections, one for each case where each block is analysed and conclusions arrived to. This structure is utilised in order to separate the two individual contributions by the authors. This allows for an individual evaluation of the authors and their achievements.

The part named "Overall Assessment" combines the findings from the three blocks from each case. Initially a summary of the findings is presented. Given the comprehensive nature of the thesis there is a need for a summary in order to facilitate for the reader. The authors are aware that this is a repetition. However, given the comprehension there is a risk that the reader either misses out on, or forgets, essential information. It might be possible to have a section referring to other parts in the thesis instead of the summary. This is however identified as inconvenient and does not fulfil the purpose of a summary.

Following the "Summary" under "Overall Assessment" the thesis presents the conclusions for each case. The three protective measures are here brought together and analysed whether or not they enable dynamic use of trade secrets.

The section called 'Business Perspective' follows the 'Summary'. The authors have found it necessary to put the findings made into a business context. The reason for this is that the nature of the thesis focuses on the possibility for companies to utilise trade secrets in a dynamical way. Under this section the findings that are strictly relating to business considerations presented.

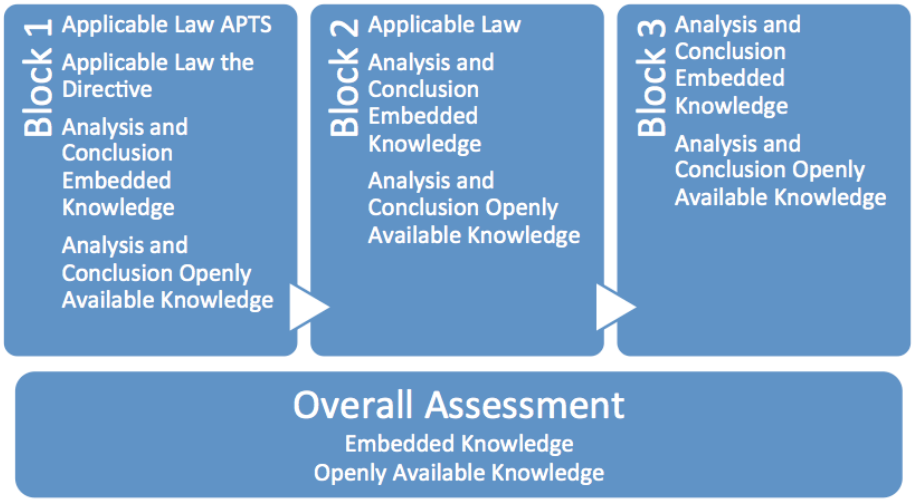


Figure 1 - Flowchart

4 Delimitations

First and foremost, the authors are well aware that it is not feasible to set up operational platform given the limited time for this thesis, why only a foundation for such a platform is the aim for the thesis. This thesis addresses only certain articles, in this case article 1 and 2 of the FHL and 2 and 3 in the Directive. The articles 3-14 of the FHL and 4-20 of the Directive will not be accounted for since they are not relevant for how to protect the trade secret, but rather works as preventive pressure not to infringe. Article 7 and 9 of FHL will be briefly touched upon for comparative purposes.

This thesis addresses none of the four IPRs, i.e. patents, trademarks, design rights, or copyright. In the case of patents and trademarks they fall outside the scope of the thesis since their nature implies disclosing the knowledge. However, patents will be used for comparisons to highlight strengths and weaknesses of the foundation of the platform. Moreover, copyright protects the representation as such from copying, and not the knowledge within, why it is not a part of the thesis either. The protection offered by design rights might be an interesting way to protect embedded knowledge, however, this protection falls outside the scope of the thesis since it does not protect the embedded knowledge but rather the design of the product.

It falls outside of the aim of this thesis to investigate the regulation for damages within the FHL and the Directive, even if these regulations might be interesting to investigate. Furthermore this thesis will not investigate the possible competition law issues. The authors identify that competition law might affect the construction of the foundations of the platform, however, it is within the scope of the thesis since the aim is to identify protection and control measures rather than other legal limitations. When creating the foundation of the platform some aspects of labour law are identified as interesting. The authors have chosen not to include these aspects since the majority of them falls outside the scope of the thesis. Moreover, the foundation of the platform is constructed from the traders' viewpoint, meaning that the employee and employer relationship generally is outside the scope. Under block 2 only Swedish law is investigated. The reasons for this is that it is not feasible due to the time period of the thesis to investigate all these issues in relation to EU-law or in relation to national law of several EU-members.

5 Theory

The following theories will be applied in this thesis: the theory of control of knowledge, the theory of the three arenas, and static and dynamic use of knowledge theory. These theories have been selected in order to put the findings into context as well as providing tools to test and falsify the findings. By applying these theories to the findings the validity of the thesis increases as well as it gives a better understanding of the complex structure and reality the findings are set in.

5.1 Petrusson's and Heiden's Theory of Control of Knowledge?

The characteristics of knowledge being infinite in the sense of scalability, creates a problem. Something that is infinitely available has no value. Therefore the reason to control knowledge is to make it scarce. When made scarce it becomes more valuable. However this is not easy which has been identified by Foray, who states that companies finds it far more difficult to control knowledge than machines.[16]

The theory that knowledge has to be controlled in order to generate value is a central theory that this thesis is based upon. The better the control the company has over its intellectual assets the easier it is to package and transact them.

5.2 Petrusson's and Heiden's Theory of Transforming Knowledge into Capital

Petrusson and Heiden make the analogy that "[j]ust as water can exist in three states (solid, liquid, gas) so can financial objects (asset, property, capital)".[17] They furthermore state that; each state of water or financial objects are bound by different characteristics and consequences that in the case of financial assets are based on the belief and trust by the economic actors. This analogy is part of a model used to explain how to better understand wealth creation within a capitalistic economy, which is dependent on the formation of capital.[18] The model furthermore shows the interplay between assets, property and capital, as shown in Figure 2.[19] The process of creating capital is a three-step process, which starts with identifying the

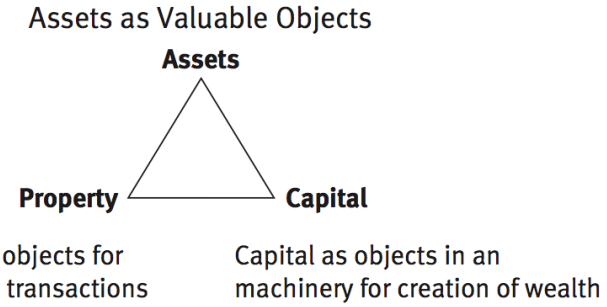


Figure 2 – Assets as Valuable Objects

[16] Foray (2004), p. 91.
[17] Heiden, Petrusson (2009), p. 277.
[18] ibid., pp. 276-277.
[19] ibid., p. 277

asset. The second step is to make the asset a property, while the third step is to capitalize on the property.

The example used by Petrusson and Heiden to explain this model is that of a house. A house is fairly easy identified as an asset, the first step. In order for the house "to be considered as property it must be trusted as an object of a commercial transaction", the second step.[20] Central for this second step of claiming the house as property is the belief in ownership rights. These rights can be validated by either the judicial system or society in general. In many countries it is fairly easy to establish that one's house is one's property, e.g. in Sweden there is a system of title deeds. However, even lack of ownership rights allows commercialization of property to occur, but it would be difficult to reach the third level; capitalisation. The requirement for capitalisation, Heiden and Petrusson continues, is that the assets have to be seen and trusted as potentially secure objects in commercial transactions.[21] For example, the house can be used as collateral for loans and bonds. If one cannot show that the house is her property it is hard, or impossible, to get a loan from the bank.

This model can be applied to intellectual phenomena, i.e. knowledge, as well, however it is a more difficult exercise than with physical assets. In the context of knowledge, the first step is to identify what knowledge is considered an intellectual asset for the firm that needs to be protected. This intellectual asset could for example be know-how, market knowledge, technical specifications or administrative data. The next step is to claim the intellectual asset as property of the firm. As with the example of the house, this is generally done through the usage of legal tools, in this case by intellectual property legislation. A company can for example apply for a patent and if granted this patent, the patent and the technical solution covered within is the company's property. By claiming that the intellectual asset falls within the criteria of an IPR the firm will establish the asset as property, which is the case where there is no administrative body, such as a patent office. This applies for example in the case of copyright. For trade secrets however, which are not considered as an IPR but are still legally protected against misappropriation, this is done by claiming the asset as a trade secret, by e.g. using non legal tools as marking it as confidential and keeping it secret. The third and final step is the difficult one. According to Petrusson and Heiden "...the asset must be trusted as potentially secure objects in commercial transactions before they can be considered as capital by financial markets, for example financing such as bonds and loans".[22] Theoretically it is fairly easy to

[20] ibid., p. 277.
[21] ibid.
[22] Heiden, Petrusson (2009), p. 277.

transact trade secrets and thereby capitalise on it, however due to the volatile nature of trade secrets and the fact that one mistake could erase the entire value, makes for a less trustworthy property for the financial markets than for instance a patent. However, this thesis will not focus on turning intellectual assets into capital. This thesis focuses on the first two steps, identification of an asset and then claiming it as property by different legal and non-legal measures. These two steps are identified as necessary to capitalise on the knowledge, which in turn can be seen as a middle ground between the property step and capital step, and that also is the aim of this thesis.

5.3 Petrusson's Theory of Controlling Knowledge in The Three Arenas

The foundation of creating the control is the communicative interaction between what Petrusson describes as the 'three arenas'. The three arenas consist of an administrative arena, a judicial arena, and a business arena as shown in Figure 3.[23] In relation to patents the administrative arena is the administrative procedures related to claiming patents, such as patent offices. The judicial arena comprises the judicial courts that are upholding the laws upon which the state is built. In relation to patents the judicial arena is mainly about validation of patents, e.g. if a competitor tries to invalidate a patent, and pursuing infringers. The business arena is described by Petrusson "as a structural platform, which in turn is a conglomerate of structural platforms, e.g. of markets, innovation systems, firms, and commercial relations".[24]

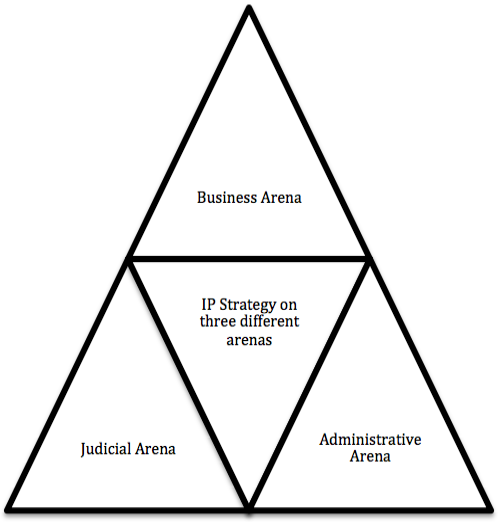


Figure 3 – The Three Arenas

The interaction between these arenas is of great importance. For example: a start-up or a SME might have been granted a patent in the administrative arena. This patent grants them a strong property claim on the patented invention. However, start-ups and SMEs do not have strong positions in the business arena due to their lack of market power. Therefore a big company might be able to use this patent because of their market power in the business arena is stronger than that of the start-up or the SME. Start-ups and SMEs have a much harder time allocating resources for a possible infringement prosecution in the judicial arena. This very simplified example shows that if a

[23] Petrusson (2004) pp. 104-105.
[24] ibid., p. 106.

company has a weak position in one arena it might be possible to offset by a strong position in another arena.

In some cases there is no applicable administrative arena, such as the patent offices, which is the case with copyright or trade secrets, at least under Swedish law. In the case of trade secrets Petrusson argues that "[b]ecause there are behaviours that can be considered as a violation of the trade secret regulation in the judicial arena, it is also possible to claim a trade secret as property in the business arena".[25] Lacking an administrative arena, it is in the case of trade secrets highly important to create and maintain a control position in the two other arenas.

5.4 Petrusson's Theory of Dynamic or Static IP

There are different ways to utilise knowledge within a company and with different outcomes. Petrusson has a theory about usage of IPRs, and discusses the concepts of static and dynamic IPRs. A static IPR is used to prevent others from using the IPR without authorisation, the concept originates from the right to use one's property without disturbance.[26] This is also the traditional way to look upon IPRs, as a way to block competitors. Dynamic IPRs on the other hand are a "set of tools used to assign property, license property, inherit property, utilize property as collateral and to claim property in a bankruptcy".[27] Dynamic IPRs are in other words used together with the rest of the society in different types of transactions instead of claiming static IPR to merely block others.

The same view, of static and dynamic use, can be applied even if the knowledge is not controlled via IPRs. A good example of this is IP in the form of trade secrets which can be used statically, i.e. when the knowledge is kept secret inside a firm and is protected against misappropriation by law, or dynamically when transacting it to parties outside of the firm.

[25] ibid., p. 115.
[26] Petrusson (2004), pp. 118-120.
[27] ibid., p. 119.

6 Background

In order to set the scene and to better understand the research questions and the economic environment they are set in, a background is presented in the following. The section will also address the importance of trade secrets in society today as well as how they can be controlled. Finally the section will identify the characteristics of knowledge since these characteristics play an important role throughout the thesis.

6.1 Knowledge Economy

Foray states that knowledge has always been at the heart of economic development.[28] However there has been a paradigm shift from the industrial economy to what is known as the Knowledge-based economy (henceforth referred to as KBE). Recent statistics from OECD shows that investments in knowledge-based capital (henceforth referred to as KBC) has exceeded the investments made in tangible capital, see Figure 4.[29] Similar statistics show that in Sweden and the United Kingdom the investments in KBC matches or exceeds the investments in tangible capital.[30] Another indication of the shift towards the KBE is the change in market-to-book-value that has taken place for the Standard & Poor's 500 companies. Market-to-book-value is the ratio of the capital market value of companies to the net asset value as stated in the companies' balance sheets and Standard & Poor's 500 is a stock market index based on the market value of the 500 largest companies in the United States. This has continuously risen since the 1980s and with a value of around 7 US year 2000 implying that for every 7 USD of market value only 1 dollar appears

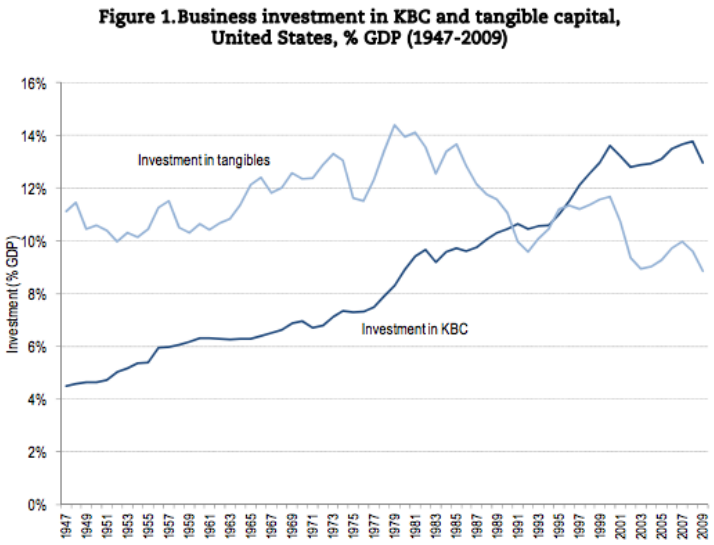


Figure 4 – Business investment in KBC and tangible capital

[28] Foray, Dominique, The Economics of Knowledge, 1st Edition, Massachusetts Institute of Technology 2004, p. 21.
[29] OECD, New Sources of Growth - Knowledge-Based Capital Driving Investment and Productivity in the 21st Century, May 2012, p. 4.
[30] ibid., p.5.

in the balance sheet and the remaining 6 USD are intellectual assets.[31] According to Petrusson and Heiden "the industrial economy is typified by a relatively few, well-known commercial means from which to create and extract value through the production, distribution, and sales of physical goods".[32] The KBE[33] on the other hand, as described by Petrusson, is an economy in which the production of physical goods does not generate sufficient wealth, but rather in the KBE "[h]uman resources have to be leveraged not only into physical products, but also into virtual products and license offers".[34] Firms in a KBE are more dependent on exploiting economies of scale through the use of intellectual property.[35] The transition from an industrial economy to the KBE can be shown in a four-step model, which is captured in Figure 5, where the value addition of knowledge and the control of it is growing with each step.[36]

The two grey boxes represent the industrial economy. In the first box competitive advantage is generated through the vicinity to natural resources. The value addition of knowledge is very low and it is therefore little need to control it. The second box illustrates that knowledge is more relevant than before since competitive advantage was generated by applying knowledge to work and production. Here it was necessary to have control over the knowledge companies possessed on how to produce the products. The third box highlights the era that many companies today are active in. Here knowledge has a very high value-addition and is therefore important to control. A typical situation is a company with

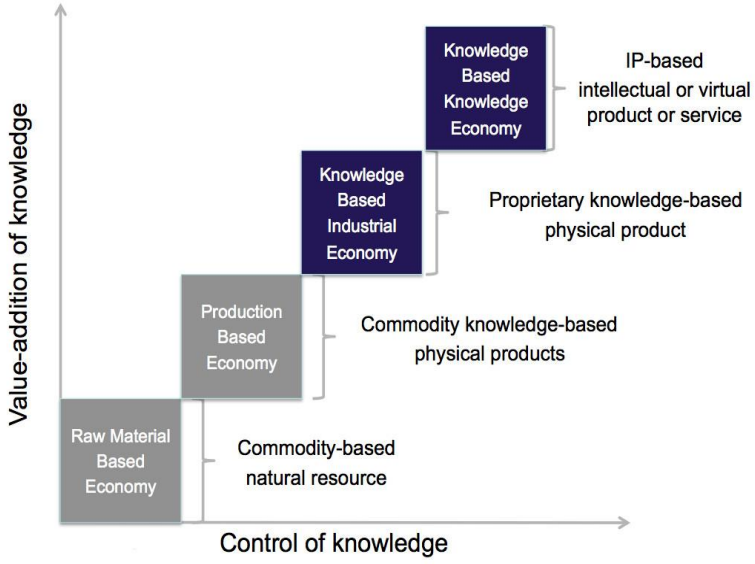


Figure 5 – Four Boxes

[31] Lev, Baruch, Intangibles: management, measurement and reporting, 1st Edition, Brookings Institution Press, Washington, D.C. 2001, p. 8-9.
[32] Heiden, Bowman J., Petrusson, Ulf, Assets, Property, and Capital in a Globalized Intellectual Value Chain, From Assets to Profits: Competing for IP Value & Return, 2nd Edition, John Wiley & Sons Inc, New Jersey 2009, p. 281.
[33] Petrusson uses the term intellectualised economy, however, the same phenomenon is intended.
[34] Petrusson, (2004) pp. 2-3.
[35] ibid.
[36] Heiden, Bo, Defining Knowledge-Based Business - The Firm, The Market, and Competitive Advantage, CIP 2013, p. 36.

proprietary technology, e.g. a patent, which is used when producing a physical product and thereby adds value to the product. The fourth and final box captures when knowledge in itself is the commodity that generates value when used in a service or virtual product. With this identified it should be mentioned that many companies today are active in both the third and the fourth box. For example when a company uses their proprietary knowledge to manufacture products, they are performing an activity related to the third box. However when they license patents and other IP or IPRs to third parties they are active within the fourth box, or as called in this thesis, the KBE.

6.2 Importance of Trade Secrets

Trade secrets imply a competitive advantage for the proprietor. This advantage might be of a first-mover character or of any other type. Studies, as presented below, show that trade secrets are important for companies. A study based on US data suggests that "enterprises in highly knowledge-intensive industries like manufacturing, information services, professional, scientific and technical services, and transportation accrue between 70% and 80% of their information portfolio value from secrets".[37] Furthermore a recent research paper from Fontana et al. (2013) shows that only 10 % of important industrial innovations are patented, suggesting that the remaining rely on secrecy or other type of competitive advantage.[38] In a survey commissioned by the European commission 75 out of 223 (34 %) respondents reported that their trade secrets had been stolen at least once.[39] A survey conducted by PWC in 2012 shows that the total cost in a worst case scenario on average, related to security incidents such as theft of trade secret, is estimated to £110,000 - £250,000 for large organisations.[40] According to a German article the financial damage caused, due to misappropriation of trade secrets in Germany, is approximately 20 - 50 billion euros.[41]

Trade secrets are furthermore vital in collaborations. In a collaboration setting, the collaborating partners often have to share their trade secret in order to develop new knowledge. A survey shows that the lack of protection of confidentiality or intellectual property was the factor identified as the most important barrier to enter into collaborations.[42]

---

[37] Forrester Consulting, The Value of Corporate Secrets: How Compliance and Collaboration Affect Enterprise Perceptions of Risk. Study carried out on behalf of RSA and Microsoft, March 2010, p. 5.

[38] Fontana et al. (2013). Reassessing patent propensity: evidence from a data-set of R&D awards 1977-2004, p. 10.

[39] European Commission, Commission Staff Working Document Impact Assessment Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Brussels, 28.11.2013, p. 17.

[40] PWC, Information security breaches survey, Technical Report, April 2012, p. 17.

[41] Weber, Industrial espionage threatens German companies and jobs, DW.DE 29.6.2010.

[42] GE & Strategy One (2013), GE Global Innovation Barometer 2013, Global Research Report, 2013, p. 5.

6.3 Trade Secrets as Means to Protect Knowledge

The exclusivity granted by an IPR does not apply for trade secrets. However, there are still numerous reasons for using trade secrets as protection for knowledge. One reason is that it might be too expensive to seek IPR protection, another that the there is no limitation in time of a trade secret. Another reason, which probably is the most common, could be that trade secrets are the only protection available.

The protection of knowledge as trade secrets is different around the world. In EU the protection differs between the Member States to a high extent. Sweden is for example the only EU-member that has an explicit trade secret act. This fragmentation of the level of protection within the EU lowers the incentives to undertake cross-border economic activities, such as trade with trade secrets and enter research collaborations, both within the country and for cross border activities, thereby lowering the trade secret based competitiveness of European businesses and research bodies.[43] As a response to this the European Commission has proposed a directive for the harmonisation of trade secret legislation throughout the EU, henceforth called 'the Directive'. Adopting the Directive would provide significant positive benefits both in terms of predictability of the law between different countries as well as in many cases raising the level of protection overall.

Before drafting the Directive, EU commissioned a study that investigated how trade secrets are protected globally. Three countries of the ones investigated stand out; USA, Japan, and Sweden. These countries are the only ones, of the investigated countries, that have explicit trade secret acts with a legal definition of what a trade secret is. Therefore the Directive has been influenced by the solutions in these countries. Hence it is no surprise that the Directive to great extent is very similar to the FHL when it comes to both structure and content. The Swedish government has confirmed this.[44]

[43] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Brussels, 28.11.2013, p 5.

[44] Justitiedepartementet, Faktapromemoria 2013/14:FPM42 Direktiv om företagshemligheter, 20.12.2013, p. 1.

6.4 Characteristics of knowledge

Knowledge has different unique characteristics compared to physical goods, which will be described in the following.

6.4.1 Non-rival

One of the main features of knowledge is that it is non-rival, sometimes called non-scarce, in the sense that it can be in two or more places at the same time. Physical, human or financial assets on the other hand are rival, or scarce, as they cannot be in more than one place at the same time. According to Lev this scarcity is shown in the cost of using such assets, a cost that reflects the missed opportunity, i.e. the next best alternative for using the asset.[45] Lev continues to say that the opportunity cost for knowledge is many times zero, or at least very low, as there is no opportunity being missed or nothing given up.[46] One contributing factor to the non-rivalry of knowledge is that once it has been developed, which might be costly, the marginal cost for using it is either zero or very low.[47] For instance it might be expensive to develop an app for a smartphone, but distributing it on the other hand is very cheap. The non-rivalry of knowledge is the main value driver as it allows for the knowledge to be sold an infinite amount of times.

6.4.2 Scalable and Cumulative

Unlike physical goods knowledge is cumulative. Machines deteriorate and must be replaced while knowledge and ideas build on the last knowledge or idea. As Foray puts it, knowledge can be seen as an intellectual input that enables creation of new knowledge and therefore broadens the spectrum of future actions.[48] Furthermore knowledge is theoretically infinitely scalable. Manufacturing physical goods is limited in proportion to the availability of resources while knowledge on the other hand is not subject to this limitation. The value creation potential of knowledge – the scalability – is generally limited only by the size of the actual market.[49]

6.4.3 Non-reversible

Knowledge is unlike physical goods non-reversible. If a physical good is given or transacted from one person or business to another, the exact same good can be retrieved. This does not apply to knowledge. When knowledge is given from one person to another it cannot be retrieved since it resides in the minds of humans.

---

[45] Lev (2001), p. 22.
[46] ibid.
[47] ibid.
[48] Foray (2004), p. 16.
[49] Lev (2001), p. 26.

6.4.4 Tacit or Explicit

Knowledge can either be tacit or explicit. Tacit knowledge is knowledge that is neither articulated nor codified. This knowledge resides in people, institutions, or routines. This characteristic also poses a problem since it makes it hard to transport, memorize, recombine, and learn the knowledge.[50] Tacit knowledge can for example be the skill an individual worker has refined over the years. Explicit knowledge is knowledge that can be codified and articulated. An example of this is schemes of how to build a physical good.

6.4.5 Non-Excludable

Foray identifies that one of the characteristics of knowledge is that it is "non-excludable".[51] What this implies is that knowledge is very difficult to make exclusive or private, i.e. it is difficult to exclude others. One way to do this is to keep the knowledge a secret, but as soon as the secret is revealed, the proprietor loses the exclusiveness and control. This characteristic differs from the one of physical goods that can be shown but the proprietor still has the control and exclusiveness of the good. This is to some extent offset by IPRs as they can give the owner an exclusive right to use the knowledge for the duration of the IPR. The hardship to make knowledge exclusive gives rise to spill over effects that benefits third parties, since they get access to expensive knowledge for free.

[50] Foray (2004), p. 18.
[51] ibid., p. 91.

7 Two Cases

This thesis will, in order to create the foundations of a platform for dynamically utilising knowledge through the three blocks, use two cases. They will be described in the following along with the imminent risks that are identified in relation to dynamic use of trade secret in each case.

7.1 Embedded Knowledge

The first case surrounds a physical product that can detect if the bearings are operating and performing as they should. SKF has today a well developed after sales market where they sell similar products. Clients who buy bearings also have an opportunity to buy products that help them detect whether or not the bearings are operating optimally, so that they can be replaced or repaired before a costly stop in operations occurs due to broken bearings. However, this thesis will investigate a product that is not yet developed but might be in the future. The reason for this is that today's products are already known by many actors and it would not provide deep and innovative conclusions. The product is a machine condition indicator, hereafter referred to as "the sensor", which can wirelessly transmit various data extracted from the bearings such as temperature, frequency, velocity, and acceleration, see Figure 6.[52] The sensor can either be mounted on a machine containing the bearing or be embedded inside the bearing if the bearing is big enough.

Figure 6 – The Sensor

Looking at a simplified section of the sensor it is seen that it consists of several different components that have to be placed in a certain way to function properly, see Figure 7. What components and how to create the sensor are the results gained through R&D at SKF. The knowledge of how to create the sensor and which components to use are not directly visible for anyone since it is embedded within the sensor, therefore the term

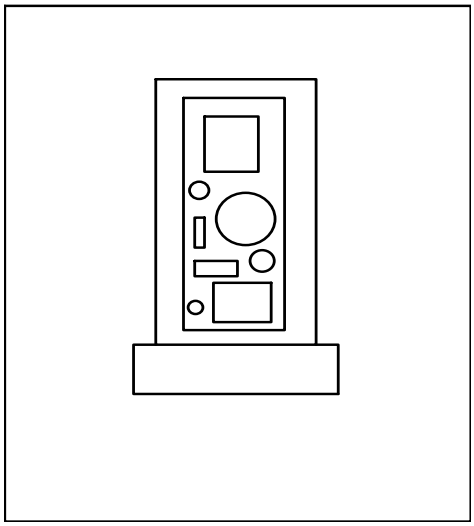


Figure 7 – Simplified Section of the Sensor

[52] SKF, "SKF Machine Condition Indicator – CMSS 200-25-PROMO Machine indication bundle", retrieved 02/06/2014 from: http://www.skf.com/binary/12-137467/CM5120%20EN%20MCA%20and%20MCI%20Promotion_tcm_12-137467.pdf

'embedded knowledge'. The blueprint is of course very simplified but serves as a tool for the reader to understand what knowledge is referred to. This knowledge, how to construct the sensor, is in this case assumed to be SKF exclusive.

7.1.1 Risks

In this section the thesis will highlight the imminent risks associated when dynamically utilising embedded knowledge.

The underlying threat in the case with embedded knowledge is that the customer gets access to the knowledge within the sensor and thereby learns it and destroys its status of being secret. Compared to the openly available knowledge case, that case implies that the customer needs to interact with the information itself in order to fulfil the task solved by the information. In the case with the sensor the aim is to stop the customer from interacting with the sensor giving the cases starting points.

7.1.1.1 Dismantling the Sensor

When transferring the sensor the trader will possess the sensor. The sensor, as shown in Figure 6, has a simple 'shell' made of plastic material that hinders the trader from readily acquiring the knowledge within. The most imminent threat in this case, is that the trader opens the case and accesses the information. By simply dismantling the sensor the can acquire the information on how to manufacture and what components to use in order to create the same sensor herself. The trader can also use this information in order to destroy the trade secret by making it accessible for any interested party.

7.1.1.2 NDT

The trader can also acquire the information within the sensor without dismantling it. Companies use today several different methods when conducting Non-Destructive testing (henceforth referred to as NDT). NDT is a wide group of analysis techniques used in science and industry to evaluate the properties of a material, component or system without causing damage. The trader may X-ray, or similar, the sensor in order to acquire some of the information within the product.

7.1.1.3 Transfer

One of the risks is that the trader who acquires the sensor transfers the sensor to a third party. This is potentially a dangerous situation since the sensor might end up in the hands of SKFs main competitors, or in any other third party's hands.

7.1.1.4 Bankruptcy

In a situation where the buying trader goes bankrupt there is a risk that the trade secret ends up in a third party's hands. In a bankruptcy situation the official trustee's main responsibility is to make sure that the creditors are reimbursed. In order to do this, the official trustee is often forced to sell all the assets the bankruptcy estate owns. This means that there is a risk that the sensor is sold to a third party in order to reimburse the creditors. Moreover, it is identified that in a worst-case scenario, a risk where the official trustee understands that she has access to a trade secret that far exceeds the value of the sensor itself, sells the information directly to a high bidding buyer.

7.1.1.5 Stealing

An identified risk is that the buying trader unwillingly transfers the sensor or the information it contains to a third party. Possible situations could be that an employee of the trader steals the sensor or that the trader is subject to espionage.

7.2 Openly Available Knowledge

A customer, who was about to build a large number of wind power stations, purchased custom made bearings from SKF. In the case of wind power it is essential that the bearings are studiously installed, the slightest error can have vast effects on the life expectancy of the bearing. In scenarios like this SKF offers the customer installation of the bearings using SKF's technicians for a fee. However, in this case the client refused this and wanted a custom made manual so that they could install the bearings using their own technicians. SKF agreed to this and created a digital manual in form of a PDF specifically for this client. The manual had to be extremely detailed in order to guarantee that the client would have the possibility to install the bearings as well as SKFs own technicians would have done. Once completed, the manual was given to the client who installed the bearings correctly.

The knowledge in this case is the knowledge inside the manual of how to install the bearings in wind power stations, knowledge that stems from R&D by SKF. The manual was custom made in the sense that it is not available to any customer who wants to buy it, why the knowledge is assumed SKF exclusive. The difference between the two cases is the way the knowledge is manifested, in the other case there is a physical product that can be held and looked upon without getting access to the knowledge inside, in this case there is a manual which, once accessed, gives access to all the knowledge of how to install bearings by reading the document. The case was that SKF transferred a digital manual to the customer, but in order to give a more general applicability of the findings, this thesis will analyse both the case of a digital manual as well as an analogue manual printed on paper.

7.2.1 Risks

In the following the most imminent identified risks will be discussed and further on in the thesis how and if it would be possible to avoid these risks using any means available, i.e. both legal and non-legal tools.

In the case of the manual it was given to the customer, however, to give the bigger picture, the risks and solutions will be reviewed from the perspective that it would be given or sold, as well as from the perspective that it is licensed out and should later be returned to SKF. When no distinction is made between business models, i.e. when the reasoning is applicable to either selling or licensing, general wording such as 'transfer' will be used. The same applies to the medium of the manual, when not further specified both digital and analogue manual is intended.

When transferring a manual to a customer in a case like this, the biggest risk that you, as a proprietor of the knowledge within the manual, take is the risk that the knowledge within the manual becomes publicly available. If that happens it implies that the competitive advantage from the manual might be lost completely, and the business unit installing bearings might face immense competition.

7.2.1.1 Too Much Information

There is one overall risk with the manual that, if solved, would solve most other issues in relation to the manual: the fact that the manual contains "too much" information. When making the manual for the customer to be able to install the bearings there is a balancing act to be made, on one hand the manual has to present enough information so that the bearing can actually be installed, while on the other hand SKF would like to limit the information within the manual so it does not pose a risk if lost or revealed. If the information in the manual is not complete for installing the bearing the value of it would be significantly lower, but also the risk when transferring the manual.

7.2.1.2 Keeping the Manual

The customer already has access to the information, however, in order to keep it, there is a need to make some sort of copy that can be kept or by simply keeping the manual instead of returning it in a licensing situation. The ways identified that some sort of copy can be made are presented in the following.

7.2.1.2.1 Photographing

Regardless if the manual is shown on the screen of an electronic device such as a computer, tablet, or is analogue and printed on paper, there is the risk that a person that has access to the manual might take photographs on one or more pages of the manual.

7.2.1.2.2 Screenshot

For a digital manual also the risk that someone might make a screenshot on one or more pages when having the file with the manual open on the computer or tablet or similar.

7.2.1.2.3 Printing

For a digital manual having the manual there is a risk that the manual may be printed onto paper and then later distributed to numerous people. Even if the computer, where the digital manual is stored, is offline and does not have any connection to a printer, it is difficult to prevent customers from merely bringing a printer to the computer and print the manual.

7.2.1.2.4 Recording

There is a risk that the persons that have access to the manual might read the information within it out loud and make a recording that is kept, either as a recording or as a transcription.

7.2.1.2.5 Copying

There is always a risk that someone who has access to the manual takes a notepad or a computer and simply copies the manual by writing off the wording inside. In relation to an analogue manual there is also the risk that a photocopier is utilised to copy the manual.

7.2.1.3 Transfer

Below is presented the possible ways the manual could be transferred from the customer to a third party. Either the manual has been copied in some way, possible ways for copying a manual have been mentioned above in relation to Keeping the manual, or the original manual is transferred.

7.2.1.3.1 Sending

Sending a digital manual can be done in numerous ways, where the most obvious one would be as an attachment to for instance an email or a Facebook message. There is also the issue that the file could possible be uploaded to a server which one or more third parties have access to and be sent that way. Also the manual could simply be transferred to an USB-memory or similar and then be transferred to a third party via that USB-memory.

For an analogue manual it would be possible to simply send it by regular mail, faxing it, using a courier or handing it over from one person to another.

7.2.1.3.2 Stealing

Having a virtual manual theft would be by hacking the device where the manual is or unwarrantedly grabbing the device where the manual is stored and walking away with it. An analogue manual would also be stolen by that someone unwarrantedly grabs the manual and then walks away with it. It

should however be noticed that the term 'stealing' is most likely not the correct one when discussing intellectual phenomena like a digital manual, since it is most likely not possible to see information as an object itself under Swedish law in which case it would not be possible to be convicted for stealing it.[53] The term stealing will be used nonetheless as it for a reader is obvious what sort of actions is referred to, and because for an analogue manual it is correct, even if it is not correct usage of the term from a legal perspective in case of a digital manual.

7.2.1.4 Learning the Information

If the manual is only licensed to the customer, there will be a time when the manual with the information within it should be returned to SKF. If, by the time it should be returned, one or more employees have learned the information within the manual this poses a risk for SKF, as SKF has no longer control over the information within the manual. This information can then be transferred from the employees to other parties and thereby pose a big threat to SKF.

7.2.1.5 Bankruptcy

If the customer enters into bankruptcy the question is what will happen to the manual, will SKF be able to remain in control over the manual or will it end up in a third party's hands. When bankrupt it is the official trustee's responsibility to reimburse creditors, which is generally done by selling assets the bankruptcy estate owns. This implies that there is a risk that the manual ends up in the hands of a third party, which might not be intended.

[53] Wainikka, Christina, Information som självständigt objekt, SvJT 2003 s 577.

8 Block 1 - Trade Secret Protection

The first block investigates the protection offered by the FHL and the Directive to see whether the knowledge in the two cases falls under this protection and what level of protection is granted. Finally an analysis will be performed addressing whether the FHL and the Directive provides sufficient control for dynamically using trade secrets for the two different cases.

8.1 Protection Offered by FHL

The FHL (1990:409) has in its first article a legal definition of what should be considered as trade secrets. The first article, as translated by WIPO, states the following:

"*For the purposes of this Act, a "trade secret" means such information concerning the business or industrial relations of a person conducting business or industrial activities which that person wants to keep secret and the divulgation of which would be likely to cause a damage to him from the point of view of competition.*

The term "information" comprises both information documented in some form, including drawings, models and other similar technical prototypes, and the knowledge of individual persons about specific circumstances even where it has not been documented in some form." [54]

There are three prerequisites that need to be fulfilled in order for knowledge to be considered a trade secret according to the legal definition, 1) it has to be considered information concerning the business or industrial relations of a trader, 2) the trader should want to keep the information secret, and 3) that the divulgation (henceforth this term is replaced by the term 'disclosure') of the information would cause damage to the trader from a competition point of view.[55]

8.1.1 Information Concerning the Business or Industrial Relations of a Trader

Fahlbeck breaks down the first prerequisite into three criteria that individually need to be fulfilled, 1) it has to be considered as information, 2) this information need to concern business or industrial relations of a trader, and 3) the holder of the trade secret need to be considered a trader.[56]

8.1.1.1 Information

According to the propositionen preceding FHL the term "Information" should be used as in regular parlance and work as a neutral collective denomination for information, knowledge and know-how

[54] "Sweden - The Act on Protection of Trade Secrets (1990:409)", retrieved 10/02/2014 from: http://www.wipo.int/wipolex/en/text.jsp?file_id=241716.

[55] Regeringens proposition om skydd för företagshemligheter 1987/88:155 p. 34.

[56] Fahlbeck (2013), p. 296.

of any kind.[57] The propositionen continues with stating that information should be given a wide meaning and can be either complex, straightforward or otherwise qualified, and can be either documented or reside in the minds of humans.[58] This has been verified both by Tonell and praxis.[59] In NJA 1998 s. 633 it was explicitly stated that there should not be any quality requirements for information to be considered trade secrets. Tacit information, however, that resides solely in the minds of the employees and that cannot be transferred to a third party, i.e. personal skill etc., is not covered and cannot be considered as trade secrets.[60] Wainikka therefore concludes that the important distinction is not whether the information is documented, i.e. has a carrier, or communicated, but rather if it is *possible* to be documented or communicate the information. If it cannot be documented it cannot be a trade secret.[61] The information can be about solitary commercial business activities, or about business activities of more general kind such as manufacturing methods, construction drawings, price determination calculations, customer lists, etc. and be documented in many different ways such as a prototype, or be stored on computer memories.[62] In other words, a trade secret can be intangibly as well as tangibly manifested.[63]

8.1.1.2 Business or Industrial Relations

To be considered a trade secret, the information must concern business or industrial relations of a trader. Both by Helgesson, Wainikka (former Helgesson), and praxis this has been interpreted as that the information must be linked to a company and the economic activities within the company.[64] According to the propositionen the term includes, but is not limited to, single commercial data, agreements made with clients, as well more common information such as market research, information that can be attributed to on-going operations, production, construction, research and development.[65] Fahlbeck states that information generally occurring is not covered.[66] Another way to

[57] Fahlbeck (2013), p. 296.
[58] Ibid.
[59] Tonell (2012), p. 22; NJA 1998 s. 633.
[60] 1987/88:155, p. 34-35; Wainikka, Christina, Företagshemligheter: en introduktion, Upplaga 1, Studentlitteratur, Lund 2010 pp. 17-18.
[61] Wainikka (2010) p. 18.
[62] 1987/88:155 pp. 65 & 35.
[63] ibid., p. 12.
[64] NJA 1998 s. 633; Helgesson (2000), p. 275; Wainikka (2010), p. 36.
[65] 1987/88:155 p. 35.
[66] Fahlbeck (2013) p. 310.

express this, according to Fahlbeck, is that the information must be of such character that revealing it would imply damage for the trader by negatively changing the trader's competitive ability.[67]

8.1.1.3 Trader

A trader, according to both the propositionen and Wainikka, is any physical or legal person that in a professional manner conducts business, regardless of whether or not the business aims at making profit.[68] This implies that not only private companies are considered traders in a legal sense, but also public authorities etc. to the extent they are conducting economic activities.[69]

8.1.2 Secrecy

Fahlbeck breaks down the second prerequisite into three separate aspects that need to be fulfilled for the information to be considered secret, 1) the time factor 2) the circle of people, and 3) the activity criteria.[70]

8.1.2.1 The Time factor

All IPRs have a limit in time, a patent is for instance only valid for 20 years, trade secrets on the other hand are not subject to this limitation as long as the other prerequisites are fulfilled. This was the issue in the case NJA 1999 s. 469 which concerned a bank and its internal instructions on how to grant credit to its customers. At the time of the trial the instructions were ten years old and the plaintiff therefore argued that they were not relevant anymore. The bank claimed that the instructions were still secret and the court was of the same opinion and stated that it does not matter how old the instructions are or if they have been replaced by new ones to consider them as trade secrets.

8.1.2.2 Circle of People

For information to be protected as trade secrets there is a requirement for the trader to keep the information secret. However, as the propositionen states, the secrecy requirement is not absolute, it can be known by several persons as long as it is not publicly available to anyone who might be interested of the information.[71] This has been verified both by praxis, Wainikka and Helgesson.[72] The secrecy requirement is hence a relative one, where the size of the circle of people that knows the

---

[67] ibid. p. 311.
[68] 1987/88:155 p. 34; Wainikka (2010) pp. 39-30.
[69] 1987/88:155 pp. 34-35.
[70] Fahlbeck (2013) p. 315.
[71] 1987/88:155 p. 35.
[72] NJA 1998 s. 633; Wainikka (2010) p. 40; Helgesson (2000) p. 296.

information is not the determinant of whether it is deemed secret or not.[73] The propositionen states that at least as long as the information is not outside the circle of people who need the information to fulfil their work it remains secret.[74] However, even information that is distributed outside the company, e.g. to a collaboration partner or in a license scenario, can maintain the secrecy status if the information is distributed only to a closed and identifiable circle.[75] The case Ö 4004-09, as referenced by Fahlbeck, points at this where the situation was that the trader A claimed that certain information, source codes, that belonged to trader B had lost its character as a trade secret since the Trader A and a person who was participating as an expert in the arbitration process knew about this information. For any other third parties the information was however unknown. The court ruled that even though these two entities knew about the information it was not reason enough to deem that the information had ceased to be secret.[76]

In relation to selling a product containing trade secrets Fahlbeck quotes SOU 1983:52, which states the following: "Moreover it seem clear how the characteristics of a secret can cease if it proliferated enough. This can happen by introducing the secret to the market, publishing it, exhibition or in any other similar way, under the condition that the secret is *accessible without thorough or extensive examination of persons skilled in the art*" (authors' translation and emphasis).[77] This is also picked up by Levin, who states that: "[i]t needs to be questioned whether or not blueprints for a product that is available on the market, and that can be analysed by anyone, by for example reverse-engineering, should be considered as a trade secret at all according to the legal definition. If the information can be acquired in any other way, for reasonable costs, many indications point to that the trade secret protection has lost its status as such."(authors' translation).[78] These two quotes implies that if a trade secret embedded within a product and is very easy to access by e.g. opening the product, it is questionable whether it really was a secret in the first place.

8.1.2.3 The Activity Criterion

There is also a need for the trader to want to keep the information secret, which implies that the trader shall have the intention to keep the information only within a limited circle of people.[79]

---

[73] 1987/88:155 p. 35; Tonell (2012) p. 28; Wainikka (2010) pp. 40-41.
[74] 1987/88:155 p. 35.
[75] ibid.
[76] Fahlbeck (2013), pp. 318-319.
[77] SOU 1983:52 Företagshemligheter. Betänkade av utredningen om skydd för företagshemligheter, p. 228.
[78] Bernitz, Ulf, Ramberg, Jan, Edenman, Ann-Charlotte, Festskrift till Jan Ramberg, 1st Edition, Norstedts juridik AB, 1997, p. 376.
[79] 1987/88:155 p. 36.

Helgesson calls this the activity criteria and it is not very severe, it is only required that the trader has a will to keep the information secret and that he has taken some sort of measure to ensure this.[80] The activity criteria has hence both a subjective dimension, i.e. the ambition to keep the information secret, and objective dimension, i.e. any activities to implement said ambition.[81] Fulfilling the criteria can be done by telling employees how to handle the information, security routines or marking documents as classified, however, it should not be considered as form prescribed by law.[82] In the case T8471/99 both the subjective and objective criteria are addressed and the court states that "the requirement for secrecy activities should not be particularly high" (authors' translation). The case was about blueprints for ships where the trader that had made the blueprints had expressed that he should retain title to them. Objectively the trader had not expressly demanded secrecy but it was customary in the line business that blueprints were kept secret. With this as background the court expressed that the defendant "should have understood that the blueprints were not allowed to be distributed or used in any other context than that where one got hold of them" (authors' translation). This case indicates that the activity criterion has low requirements and that customs in the line of business affects the activity requirement.

A contrasting case is the case called "Factoringmålet" (AD 2013:24) where the labour court stated that "information can per se be secret even if given to persons outside the company. The information can however not be proliferated for an all too big and unidentified circle" (authors' translation). In the case the information was not deemed as a trade secret since the trader had not fulfilled the requirement of clarifying that it was secret. Tonell raises the issue that the burden of proof is upon the party that disclosed the information that it is in fact secret, why being thorough in protecting the firm's trade secrets is advisable even though there are low requirements.[83]

8.1.3 Damage

Fahlbeck breaks down the third prerequisite into three aspects 1) that the disclosure is *likely* to cause damage from a competition point of view, 2) for which trader the damage should be likely to be caused, and 3) what is understood with damage from a competition point of view.[84]

[80] Helgesson (2000) pp. 296-297.
[81] Fahlbäck (2013) p. 323.
[82] Helgesson (2000) pp. 296-297; 1987/88:155 p.36; Tonell (2012) p. 29.
[83] Tonell (2012) p. 29.
[84] Fahlbeck (2013), p. 327.

8.1.3.1 Disclosure Likely to Cause Damage

By the third requisite it is implied that the information must be valuable for the trader. Tonell describes this as that the information has such commercial value and relevance that disclosure of the trade secret would affect the competitive strength of the trader.[85] There is however no requirement that financial damage has actually occurred in the specific case, which is demonstrated by the word "likely" in the article, but rather if revealing the trade secret in that situation typically causes damage.[86] Furthermore, when valuing whether revealing trade secrets could have caused damage in the specific case it is irrelevant whether or not the information was costly to obtain, but rather if the actual revealing has caused financial or other damage for the trader.[87] In article 9 of the FHL it is said that "for a violation of the trade secret of a Trader, consideration shall also be given to his interest that the secret is not exploited or revealed without authorization and to other circumstances of other than purely economic importance". (authors' translation). This shows that the damages do not only have to be of economical character.

8.1.3.2 For Which Trader

According to Fahlbeck it is generally easy to answer the question for which trader the damage is likely to be caused, in most cases the information is only available for the trader that is the creator and in such case it is for this trader the damage is likely to be caused.[88] However, a trader might get access to another trader's trade secrets by, for instance, a license deal or in a collaboration setting. However, it does not mention if this is possible where a trader purchases the trade secret. The propositionen says that in such a case the trade secret can be seen as mutual between the two traders, and if the trade secret is revealed both traders are usually afflicted.[89] In some cases, even if the trade secret is mutual, only the trader from whom the trade secret stems is afflicted, in which case it is still protected by trade secret law, in terms of damages and penalties, even though another trader has revealed it and is no longer a trade secret according to FHL.[90]

---

[85] Tonell (2012), p. 32.
[86] 1987/88:155, p.36; Tonell (2012), p. 32, Wainikka (2010), p. 42.
[87] 1987/88:155, p. 37.
[88] Fahlbeck (2013), p. 328.
[89] 1987/88:155, p. 37.
[90] 1987/88:155, p. 37.

8.1.3.3 Damage From Competition Point of View

According to the propositionen this criteria implies that only relevant information may be protected as trade secrets.[91] In other words, only when disclosure would negatively change the trader's competitiveness it is relevant. This aspect has been addressed in the case NJA 1995 s. 347 where the question was whether or not the internal instructions of a bank were to be seen as trade secrets. The Supreme Court noted that the purpose of having the instructions were to give the employees regulations for how to act in the case of unauthorized withdrawals. Thereafter the court stated that these regulations affect the bank's possibilities to compete on the market and should therefore be seen as trade secrets. The Supreme Court furthermore mentioned that even if some external actors know the regulations, i.e. other banks, and the content of the bank's regulations are similar to the external actors' regulations; it is in the interest of the bank that they are not disclosed.

8.2 Article 2 - Unwarranted Use

According to Fahlbeck article 2 FHL needs to be studied together with article 1 in order to understand the scope of FHL. Article 2 states, according to the WIPOs translation, the following:

"The Act applies only to unwarranted infringements of trade secrets.

As an unwarranted infringement is not to be considered the fact that someone acquires, exploits or discloses what is a trade secret of a person conducting business or industrial activities in order to make available to the public or before a public authority disclose something that may be an offence for which imprisonment may be adjudicated, or which may be considered to be another serious incongruity in the business or industrial activity of a person conducting such activities.

As an unwarranted infringement is not considered the fact that someone exploits or discloses a trade secret about which he or someone before him acquired knowledge in good faith."[92]

The first paragraph states the general principle that the act only covers unwarranted infringements of trade secrets while the second and third paragraph states examples of warranted infringements. An unwarranted offence can therefore, according to Fahlbeck, only be of the character where someone; acquires, exploits, or discloses the trade secret.[93]

[91] ibid., p. 13.
[92] Sweden - The Act on Protection of Trade Secrets (1990:409)
[93] Fahlbeck (2013), p. 355.

8.2.1 Acquires

According to the propositionen the term acquire relates to all sorts of acquisitions of the information.[94] The term also implies that a certain activity is necessary and that the trader, if unwillingly or by chance has acquired the information, is not liable.[95] Fahlbeck further analyses that the term means that you cannot acquire something you already possess, something new must be added to the 'infringer's' sphere.[96] In the next section he furthermore describes that it is not a requirement that the attacker takes part of the information, the attacker can for example be passive and only 'steal' the information in order to transfer it to a third party.[97]

If a trader legally purchases a product containing a trade secret and uses reverse engineering in order to acquire the information within, this is not identified as an unlawful acquirement.[98] Moreover, acquiring information this way does not mean that the information has been made public and thereby losing it status as a trade secret. The situation, according to Fahlbeck, can then be that both the proprietor of the trade secret and the trader that reversed-engineered it owns the trade secret mutually.[99] However the acquiring party can use this information anyway she wants to in her commercial activity. It is therefore possible, after acquiring a product legally, to reverse-engineer it in order to acquire the knowledge and according to FHL legally make the information publically available FHL.[100]

8.2.2 Exploits

The propositionen states the following: "[e]xploiting means that somebody, in her own business, uses the information that is a trade secret. It is a question of commercial utilisation but there is no requirement that it leads to profit" (authors' translation).[101] The prerequisite also has an activity criterion, meaning that the prerequisite is not fulfilled if the attacker just passively sits on the information. Fahlbeck states, after analysing the case Ö 9002-03, "språkcentrum-målet", decided by the Court of Appeal that if a competitor only possess the trade secret this requirement is not fulfilled.[102] Furthermore, the propositionen's statement that it has to be used commercially implies

---

[94] ibid., p. 353.
[95] ibid.
[96] ibid., p. 355.
[97] ibid.
[98] ibid., p. 403; Bengtsson, Henrik, Kahn, Johan, (2005) Företagshemligheter i domstolarnas praxis - del 2, Ny Juridik 3:05 p. 7.
[99] Fahlbeck (2013), p. 403.
[100] ibid., p. 404.
[101] 1987/88:155 p. 41.
[102] Fahlbeck (2013), p 361.

that if an employee steals the trade secret or uses it in private activity, then the employee is not accountable since this does not constitute a commercial activity. However, the meaning of commercial activity is not clear. Fahlbeck analyses this prerequisite by asking three questions: 1) Does the exploitation have to occur externally in the sense that in an investigation it can be established that the actual information has been used? The example used by Fahlbeck is if a potential customer has been contacted by the alleged infringer who then openly has been using information that is exclusive for the alleged infringed party. 2) Does the exploitation need to occur in a way so the information is actually used or is it enough that the information affects the actions so that the infringer refrains from directly using the information and acts in a different way instead? Fahlbeck's example is that of a customer register that has been abducted. Does the infringer have to contact persons within the customer register or is it enough that the infringer uses it to target different customers, i.e. as an elimination moment? 3) Is it enough that the information is used internally?[103] Fahlbeck's answer, after analysing that the propositionen does not address these questions, is that the first two questions are negative and the third positive.[104] This means, according to Fahlbeck, that exploitation does not have to occur externally, that information generally used externally can also be exploited solely for internal purposes by affecting the infringer's actions, i.e. referring to the case above, the infringer does not need to actually use the customer list since drawing inspiration from it is enough, and that exploitation can also be solely internally in the infringer's own commercial activities by for example research and development work.

8.2.3 Disclosure

It is, according to SOU 2008:63, not a requirement that the disclosure is made to a certain person.[105] It is furthermore irrelevant how the trade secret is disclosed. It can according to the SOU 2008:63 be disclosed either orally or in writing.[106] It can also be disclosed by someone handing over an object from which the trade secret can be deduced.[107]

Fahlbeck analyses what is the critical moment for disclosure. He states that in a situation where a resigning employee has access to a trade secret, and where the employee transfers this to her medium, e.g. a USB memory card, when she leaves the company, there is no disclosure since she

[103] ibid. pp. 361-362.
[104] ibid.
[105] SOU 2008:63 Förstärkt skydd för företagshemligheter, p. 319.
[106] ibid., p. 323.
[107] ibid.

transfers the information to her medium.[108] If she uses the trade secret in her own private business and conducts competing business with the previous employer this situation might be considered as an unwarranted exploitation of a trade secret according to FHL, but not as a disclosure.[109] In order for the information to be identified as disclosed according to FHL the information needs to be 1) unauthorised transferred to a new trader, e.g. the new employer of the abductor, and then either 2a) becomes known for the new trader, or 2b) the new employee, i.e. the abductor, has a position that implies that the new trader knows of the stolen information already by knowing that the abductor has the information.[110] An e contrario conclusion gives that the trade secret can be disclosed to private persons and still not be considered disclosed according to the FHL, as long as it does not become known for any legal persons.

Fahlbeck states that a trade secret may be at several traders at the same time before he asks the question whether or not the information loses it characteristics as a trade secret if any of the traders discloses the information to a third party. Differently put, does an unwarranted disclosure at the same time imply that the information no longer exists in a limited and controlled circle and thereby becomes public and is no longer a trade secret? According to Fahlbeck this question has been addressed in arbitration, however he does not refer to any specific case. Fahlbeck states the following: "Whenever the transfer of information is warranted it is undoubtedly allowed. However, when the transfer is unwarranted the answer depends on the circumstances. If it is clear that the information has been disclosed to a certain trader and she realises, or should at least realise, that it is secret information she has been given, then the information ought to maintain its character as a trade secret for all traders who has access to the information." (authors' translation).[111] The reason for still being identified as a trade secret is that the circle is still limited and controlled.

8.2.4 Unwarranted

The FHL protects only trade secrets against unwarranted offences and this has led to that it appears that the first paragraph of the article 2 has a character of a general clause. This is however no not the case.[112] Wainikka states that responsibility requires an offence to fall within the scope of either of the responsibility articles 3-8.[113]

---

[108] Fahlbeck (2013), p. 371.
[109] ibid.
[110] Fahlbeck (2013), p 373.
[111] Fahlbeck (2013), p. 322.
[112] Wainikka (2010), p. 43.
[113] ibid.

The second and the third paragraph of article 2 states examples of situations where an offence is not deemed as unwarranted. However there are other situations that are not identified as unwarranted offences. The first is according to the propositionen that the trader has explicitly or implicitly given her consent.[114] The second situation according to the propositionen, is where one has an obligation to disclose information according to law, e.g. as a witness.[115] The third and fourth situations that are not considered as unwarranted addresses employee and union exceptions. These are outside the scope of this thesis and are therefore not mentioned any further. The fifth situation regards the situation where a trader or an employee can defend their rights against a trader. The situation whether or not the employee can defend her rights or not will not be further mentioned since it falls outside the scope of this thesis. Fahlbeck analyses whether or not a trader can legally, on her own, acquire information of another trader in order to secure evidence in a legal dispute. He answers this question that it might be possible if a trader suspects that a competing trader has unwarrantably infringed the suspecting trader's trade secret.[116] The suspecting trader can get this information by demanding an employee of the infringing trader to give him the information.

The second paragraph is an example stating that someone, e.g. an employee, can disclose "something that may be an offence for which imprisonment may be adjudicated, or which may be considered to be another serious incongruity in the business or industrial activity of a person conducting such activities" (WIPO translation). This example falls outside of the scope of this thesis and will therefore not be mentioned any further. On the other hand, the third paragraph falls within the scope of the thesis. The third paragraph means that if a trader was in good faith when she acquired the trade secret, i.e. she did not know that she acquired a trade secret, and then either exploits, discloses, or acquires the trade secret, it will not be deemed as an unwarranted offence.[117] Fahlbeck analyses the situation where a trade secret has passed several different traders and comes to the conclusion that in order for the last trader to be responsible for an offence, not only does she need to have been in bad faith when she acquired trade secret but also all the intermediaries needs to have been in bad faith.[118] The outcome of this regulation is according to Fahlbeck that a trader might lose the "right" to the trade secret if it is acquired by a trader who is in good faith since the secret character of the information is extinguished.[119]

---

[114] 1987/88:155, p. 45.
[115] ibid.
[116] Fahlbeck (2013), p. 380.
[117] Fahlbeck (2013), p. 395.
[118] ibid., pp. 395-396.
[119] ibid., p. 396.

8.3 EU Trade Secret Protection

The 28th November 2013 the European Commission presented a proposal for a directive on a uniform trade secret protection within the EU that will be reviewed in the following. The reason for reviewing the Directive is that even though Sweden has a good protection for trade secrets in the sense that Sweden actually has an act on protection of trade secrets (FHL), Sweden is a very small country. To make this thesis more general an outlook on the proposed EU directive will therefore be done, as this will ensure that the findings in this thesis may be more or less applicable in the whole EU.

Article 2, which gives the trade secret definition, states that:

"*'trade secret' means information which meets all of the following requirements*

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) has commercial value because it is secret;

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."[120]

The identified prerequisites are information, secrecy, commercial value, and activity, which will be analysed in the following.

8.3.1 Information

A teleological interpretation gives that the term "information" must be given a wide meaning, as the purpose of the Directive is to enhance possibilities for research collaborations and trade with trade secrets. This is also supported by the Directive itself which says that regarding trade secrets a "definition should therefore be constructed as to cover business information, technological information and know-how".[121] If a narrow meaning would be adopted the Directive would not grant an effective protection of trade secrets within the EU. The Swedish trade secret act also indicates that information should be given a wide meaning. Like the FHL the Directive states that personal skills – tacit knowledge – should not be covered, however, the Directive should not cover trivial information whereas it can be covered by the FHL.[122]

[120] European Commission Proposal (2013), p. 17.
[121] ibid., pp.12-13.
[122] ibid.

8.3.2 Secrecy

A literal interpretation of the secrecy prerequisite appears to have a relative meaning just as it has in Swedish law, implying that the information may be known by more people than just the ones working with it etc. The important distinction is if the information is generally known within the circle that normally deals with this information or is at least readily accessible to this circle of people. An e contrario interpretation gives that if the information is known by everyone outside the circle and is readily available to them but not to people within the circle, then it will still be considered secret.

8.3.3 Commercial Value

The only reasonable interpretation of commercial value must be that the secret information somehow grants the holder a competitive advantage. This might be either direct, as if the information can be used to improve a product, or indirect, if the information is not valuable to the holder but would be very valuable for a competitor. This prerequisite is similar to the one in the FHL stating that "*the disclosure of which would be likely to cause a damage to him from the point of view of competition*".[123] For a disclosure to be possible, the information must be secret, and for damage to occur, the information must also have a commercial value. Therefore, even though the writing is different, the Directive seems to imply the same thing as FHL.

8.3.4 Activity

A literal interpretation of this prerequisite implies that different circumstances require different steps to keep the information secret. Therefore in a situation where the trade secret is utilised internally the demand for activity to keep it secret is most likely less, than in a situation where the trade secret is utilised externally. Furthermore a literal interpretation leads to that if the information is of high value for the person lawfully in control of it, the reasonable activity level is likely to be higher than if the information is of less value. Compared to the FHL this prerequisite expressly states that different circumstances demand different activity levels whereas the FHL only states that an activity is needed. Out of the four prerequisites this is identified as the one that differs the most between the Directive and the FHL. In Swedish case law a lack of activity has, in at least one case, been 'healed' by customs in the line of business or there has been a low level of required activity overall, something that most likely will not be the case for the Directive.

[123] Sweden – The act on Protection of Trade Secrets (1990:409) Article 1.

8.4 Scope of Protection – Article 3

Article 3 of the Directive states that that "*trade secret holders are entitled to apply for the measures, procedures and remedies provided for in this Directive in order to prevent, or obtain redress for, the unlawful acquisition, use or disclosure of a trade secret*".[124] Hence, to be granted any rights according to the Directive against actions by third parties, there are three prerequisites that need to be fulfilled first. These prerequisites are 1) it has to be a trade secret according to the definition in the Directive, 2) the action has to be considered either as an acquisition, use or disclosure according to the Directive, and 3) the action has to be unlawful. What is considered a trade secret according to the Directive has been addressed above, the other prerequisites will be analysed below. In order to read the entirety of article 3, see appendix 1.

8.4.1 Acquisition

The Directive itself gives no definition as what should be considered as an acquisition, however, it does present a list of different ways that a trade secret can be acquired unlawfully in paragraph 2, article 3. This list is has several different ways that a trade secret can be unlawfully acquired. In line with this, along with a teleological interpretation, gives that the term acquisition must be interpreted widely and hence can be done in many different ways.

For the acquisition to be considered as unlawful there is also a requirement that it is done without the consent of the trade secret holder and that it is done intentionally or with gross negligence. Where the line should be drawn between 'normal' negligence and gross negligence is however unclear and depends most certainly on the circumstances in the specific case.

One way to acquire the trade secret that, most likely, is not unlawful is to buy a product that has been put on the internal market and then use reverse engineering to see what is inside it and thereby get access to any trade secrets inside. If the buyer is under no obligation not to use reverse engineering then it is not unlawful to use this method to get access to trade secrets.

8.4.2 Use

Article 3, paragraph 5, of the Directive states that "*[t]he conscious and deliberate production, offering or placing on the market of infringing goods, or import, export or storage of infringing goods for those purposes"* should be considered as unlawful uses.[125] This paragraph then works as a specification of the more general rules given under paragraph 3, article 3. Under article 2 of the Directive is the definition of what should be considered an infringing good given, which is "*goods whose design, quality, manufacturing process*

[124] European Commission Proposal (2013), p.17.
[125] ibid.

or marketing significantly benefits from trade secrets unlawfully acquired, used or disclosed".[126] As is seen it is quite straight forward what can be considered unlawful use of trade secrets, however, this is most likely not an exhaustive list of possible unlawful uses, as it is very product focused. A teleological interpretation would give that using know-how on how to perform a process would also be considered a use according to the Directive. There is also an issue as to what should be implied by 'goods'. Does it cover only physical things or is also intellectual things covered? A teleological interpretation would give that both physical and intellectual things are considered 'goods' in the eye of the Directive.

8.4.3 Disclosure

As a trade secret is information, and by the very nature of the concept of trade secrets the information is also secret. A teleological interpretation of what should be considered a disclosure of a trade secret is therefore that it becomes known. The question, however, is when this is considered to be done, i.e. how many must the trade secret be known to in order to have been disclosed? In order for the Directive to grant a good protection, the number of persons that it becomes known to must be few, the protection would be illusory if there was a need for the information to be widely known before it would be considered as a disclosure by the Directive. Under FHL there is a requirement that the information becomes known for a trader to be seen as a disclosure, a private person would not be enough, it is however unclear if there is a similar requirement for the Directive.

8.4.4 Unlawful Use or Disclosure

For a use or disclosure to be considered unlawful it has to be done either intentionally or by gross negligence, and without the consent of the trade secret holder, according to paragraph 3, article 3. For it to be considered as an unlawful use or disclosure the person performing the action must be found to meet one of the following conditions: 1) that the trade secret was unlawfully acquired, 2) is in breach of a confidentiality agreement or similar, or 3) is in breach of a contractual obligation to limit the use of the trade secret.

According to paragraph 4 of article 3 there is another situation when a use or disclosure should be considered unlawful, namely if the person *"at the time of use or disclosure, knew or should, under the circumstances, have known that the trade secret was obtained from another person who was using or disclosing the trade secret unlawfully within the meaning of the paragraph 3".*[127]

[126] ibid., p. 17.

[127] European Commission Proposal (2013), p. 18.

9 Embedded Knowledge – Analysis of the FHL and the Directive

Following Petrusson's statement that describing information, as a trade secret is a claiming process that if accepted in the business arena, the actor has trade secrets that can be defined as an asset. The following sections will therefore analyse if the sensor, and the information it contains can be identified as a trade secret according to the first article of the FHL. It will be presented by analysing each of the three aspects of the three prerequisites. Thereafter the author will analyse whether or not the sensor can be identified as a trade secret according to the Directive. Finally the protection given by the both legislations will be analysed in relation to the imminent risks.

9.1 FHL Analysis of Article 1

The following will investigate whether or not the sensor fulfils the prerequisites found in article 1 of the FHL. The three prerequisites are divided into the three factors that they contain.

9.1.1 Information Concerning the Business or Industrial Relations of a Trader

9.1.1.1 Information

As is identified in the propositionen and in doctrine, the important distinction is that tacit information is not protected by the FHL. The FHL protects only information that can be documented. Since the blueprints, component data, technical data, manufacturing data, and etc., of the sensor can be documented, either on a piece of paper or virtually, it is established that this criterion is fulfilled. In this case the paper or the virtual file becomes the carrier of the information. The question is whether or not the sensor itself, when manufactured, can be seen as a documentation of information? Following the propositionen stating that the information regarding the construction of the sensors can be documented in a prototype implies that the sensor per se becomes the carrier of the information. This is because if the sensor is dismantled and observed a third party will gain information on how to construct the sensor and possibly its relation to the bearings. The case 1114/97 supports this view. In the case the district court of Stockholm came to the conclusion that circuitry could be seen as trade secrets. The case was appealed but the Court of Appeal never tried the question whether or not the circuitry was to be identified as trade secrets.[128] It should therefore be noticed that the case is of less judicial value since it was not tried by the Supreme Court and the relevant question was only tried by the district court. However, the case hints that the court might identify the sensor as a trade secret. The case, together with the propositionen stating that information can be tangibly represented, supports the conclusion that the

[128] Bengtsson, Kahn (2005), p. 6.

sensors can be carriers of information. Therefore it is identified that there are two situations in this case that refer to carrying information, 1) where the blueprints and the similar data is documented, i.e. embodied, physically or virtually and 2) where the sensor itself is the carrier of information. In this thesis it is the second case that is referred to when information, or the knowledge within the sensor, is discussed and analysed.

9.1.1.2 Business or Industrial Relations

To be a trade secrets according to the legal definition the information needs to concern business or industrial relations of the trader. Doctrine and case law show that this means that the information needs to be linked to an economical activity of the company. SKF is a company that does not only produce bearings but also produce – as mentioned above – products that helps the clients maintain their purchased bearings and machines, i.e. products on the 'aftermarket'. Manufacturing and selling the sensor is therefore identified as a part of SKFs business activity. Furthermore the information is linked to the industrial relations of SKF, since it shows how to manufacture sensors that can detect irregularities in bearings. It is therefore established that there is both a business relation and an industrial relation. It is recognised that the information is not generally occurring since it stems from SKFs own R&D. There is of course a risk that another company has developed the same technology. If revealed, it would damage SKF economically and affect their ability to compete negatively, because it would hamper SKF's leverage position in negotiations if the customers could either install or do the products and services themselves or buy them from competitors. Such scenario would drive the prices down and in the long run decreasing the turnover for SKF.

9.1.1.3 Trader

The third aspect, regarding if SKF is identified as a trader or not, is easily analysed. There is no doubt that SKF, being a legal entity that develops, produces, and sells products and services is identified as a trader. With all three aspects fulfilled the first prerequisite is identified as fulfilled.

9.1.2 Secrecy

9.1.2.1 The Time Factor

Considering the time factor, even if the sensor was developed several years ago, it is still considered as a trade secret. This applies even if SKF would develop a new version of the sensor later on. This conclusion is supported by the general view on trade secrets having no limitations in time and the case NJA 1999 s. 469, as referred to under section 8.1.2.1.

9.1.2.2 Circle of People

The analysis of the applicable law shows that it is of great importance to control the circle of people that has access to the information, since the secrecy requirement is not absolute but relative. During manufacture it is relatively easy to identify the circle, since it is most likely the manufacturing department that knows the secret. The question is what happens in a situation where the sensor is transacted to a customer? The analysis shows that the sensor can be distributed outside the company and still maintain its secrecy status, if it is distributed to a closed and identifiable circle. Following SOU 1983:52 and Levin's statement, that one way to lose the secret character is by introducing the sensor to the market under the condition that it is easily accessible for a person skilled in the art, shows that it might be a problem when a buyer purchases the sensor. In the case where the trade secret is sold to whomever wants to buy it, it can be claimed that the secret is not widely spread implying that it is still a trade secret, since it is heavily protected by locks or other physical tools that a person skilled in the art cannot easily access. It is however hard to know where the line is to be drawn for something that is easily accessible for a person skilled in the art since there is no case law or doctrine that point to the answer. One can speculate that if the sensor is only protected by a plastic cask and sits on top of the machine that contains the bearing, it would most likely be considered as easily accessible for a person skilled in the art. The sensor will in that case lose its characteristic as a trade secret. Another factor that might affect the outcome is whether or not the information per se is not easily accessible for a person skilled in the art. If the sensor is of technology that not even a person who is skilled in the art understand how it works, or is able to easily understand how works, one could argue that it is not easily accessible. This is not addressed in law but as shown it might be possible to use this line of argumentation. The conclusion that can be drawn is that selling the sensor to whoever wants to buy it is an unpredictable business model.

The question is what happens if the sensor is not sold but rather the right to use it is licensed and the sensor itself is leased out? When using the expression that the sensor is "licensed out", the author describes the situation where both the right to use the sensor and that the sensor itself is leased out, In order to avoid reiteration. A licensing right means that the licensor maintains the ownership rights for the sensor and that the licensee only has license rights, i.e. she is allowed to use the sensor in return for example royalty payment. The same reasoning applies where the sensor itself is leased out, i.e. no ownership rights are transferred. A licensing agreement is entered after negotiations between the parties and especially in situations like these where the agreement represent great values. This behaviour points to that it should not be considered as "put on the market", since

it is not accessible for whoever wants it. The conclusion is therefore that it is easier to maintain control of the circle if SKF negotiates with each interesting party, as is the case when conducting a licensing business model rather when utilising a sales model. Therefore a business model that focuses on licensing the sensor is identified as safer in terms of keeping the information secret.

An interesting question is if custom made products means that the product is put on the market or not. This has not been addressed in the doctrine and is therefore of a speculative nature. SKF sells their products through two different distribution channels: one where they act as an original equipment manufacturer (henceforth referred to as OEM) and sells towards these customer's directly and one where they sell to distributors, which are either owned by SKF or are independent. An OEM is "a company whose products are used as components in another company's products".[129] The companies SKF sell to can be anything from car manufacturers to wind power manufacturers. When selling to these customers there is always an element of customisation since the products always differ depending on who is the customer, i.e. BMW uses different dimensions and specifications on their products than Volvo does. The fact that these sales agreements enter into force after extensive negotiations and often runs for a long time, point to that they should not be seen as "put on the market". However, when the products are components of something that is eventually sold to a consumer, one can argue that the product is put on the market. For example in the case where the product is sold to a car manufacturer, i.e. SKF sells a bearing containing the sensor to Volvo, Volvo incorporates the component in their cars, which are eventually sold to the consumers. The consumers having bought the car are able to do whatever they want with it. It is undoubtedly so that when the car containing the trade secret is sold to the consumers, it is to be seen as put on the market. These types of sales point to that the products are not put on the market since they are so specific, and thereby might be protected by the FHL. On the other hand when SKF sells to the distributors the situation is different. When the distributors want products the place an order and sell them to whoever wants them. In this case it is certain to say that the products have been put on the market and that the product is most likely not considered as a trade secret according to the FHL, with the restriction that the information is easily accessible by a person skilled in the art. However, one could argue that when the products are sold to distributors they cannot gain the trade secret protection given by FHL since the spread of the trade secret is public and uncontrolled, making the circle is most likely not defined, limited and closed.

[129] Retrieved 07/05/14 from: http://www.investopedia.com/terms/o/oem.asp.

Following the case "Ö4004-09" it is shown that even if some actors knows how the sensor is built and what it contains, i.e. they have the exact same knowledge, it can still have a character of a secret. It loses this character first when the circle is unidentified and uncontrolled. This is an important feature since it shows that even if some actors know about the secret it does not lose its status. However, the applicable law does not point to how many actors can know about the secret before it loses its status.

9.1.2.3 The Activity Criterion

It is established, in the analysis that the protection given by the FHL does not stand on its own. Some external activity measures are required in order for the FHL to be applicable, in this case making sure that not everyone has access to the information. If the sensor was "open", meaning that anyone who passes it would see how it is constructed and what components it consist of, the circle of persons is not longer easily identified. Put in other words, there needs to be an interaction between the contractual provisions and the practical measures in order to get the protection from the FHL.

The case T 8471/99 established that it might not be necessary to have an interaction between the contractual provisions or activities such as stamps, locks, or passwords in order to be granted the protection from the FHL. This applies only if the court establishes that it is customary in the line of business to keep the information secret or that the customer should have understood that SKF wanted the information to be kept secret. The requirements for this prerequisite are, very low, why it would be recklessly not to protect it. Furthermore, a thorough use of different activities will make it easier to show that there has been a breach since burden of proof is upon the disclosing party.

9.1.3 Damage

9.1.3.1 Disclosure Likely to Cause Damage

As is established in the analysis section, it is irrelevant whether or not SKF have spent a lot of resources in order to develop and construct the sensors. However, the information is still valuable for SKF since it gives them leverage in negotiations with their buyers. With the sensor kept as a secret SKF is able to negotiate better terms. It is identified that other companies, more focused on sensors and similar products, might offer other sensors and solutions. In the case where the secret is disclosed SKFs competitive ability is hampered since these actors might offer solutions for better

terms. Therefore it is identified that there is a risk that disclosure of the trade secret would affect the competitive strength of SKF since customers might choose other solutions.

9.1.3.2 For Which Trader

In the case where SKF transfers the sensor it is shown in the analysis section that the sensor will still enjoy the protection of the FHL, in terms of damages and penalties, even if it is disclosed at a customer's site. It is furthermore identified that SKF is the trader who will suffer damage since it would hamper the competitive strength of SKF, which is analysed in the section above. A scenario where the customer suffers damage because other companies will know what technique the customer is using is identified as unlikely or in best case, not damaging at all. However, as mentioned by the propositionen, when the trade secret is licensed out it can become mutual, i.e. both the licensor and the licensee have the trade secret.

9.1.3.3 Damage From Competition Point of View

This prerequisite has been interpreted that only when disclosure would negatively change the trader's competitiveness the information is identified as relevant. This question has already been addressed in section 9.1.3.1 where it was established that it would negatively affect SKFs competitiveness. Following the Supreme Court's statements in NJA 1995 s. 347 it is also identified that even if some actors already know or have similar solutions to the sensor, SKFs sensor will still enjoy protection from the FHL since SKF has an interest that the sensor is not to be disclosed.

9.1.4 Conclusion

An overall assessment of the analysis shows that it is most likely possible to claim the sensor as a trade secret according to the FHL if actions that restrict access to the information are taken. However, if one wishes to use the sensor dynamically, by selling the sensor, protection from the FHL might not be possible. SOU 1983:52 and Levin's statement stating that if a product is "on the market" it can lose its characteristic as a trade secret if it is able to reverse engineer the product for reasonable costs, shows that it might be impossible to get the sensor protected by the FHL. One can only speculate where the threshold is for whether or not something is unreasonable costly or easily accessible for a person skilled in the art. It might be possible to address lots of different non-legal tools to the sensor, e.g. locks, stamps, etc. so that it becomes deemed as unreasonably costly to reverse engineer it. One way to get around this, and to increase the chances of keeping it secret according to the legal definition, is to license out the sensor rather than selling it. A licensing model

enables control of the circle of people knowing about the trade secret, i.e. the relative secrecy criteria of the FHL is fulfilled.

Applying Petrusson's and Heiden's theory that in order to capitalise on IA one needs to have a property claim, gives that it is possible to capitalise on the sensor. There is therefore no doubt that the sensor and the knowledge within can be claimed as property. The question whether or not this is a strong or weak property claim is elaborated around in section 9.3.5.

Petrusson's theory on the three arenas and his statement that describing a trade secret is a claiming process in the business arena shows that it is possible to claim the sensor as a trade secret, even if the FHL would not recognize it as such when it is dynamically utilised. This is possible since there is no administrative arena that regulates whether or not something is a trade secret or not, i.e. it is the trader herself who determines if it is a trade secret or not, until proven otherwise in the judicial arena. However, if not identified as a trade secret according to the definition in the FHL, the trade secret claim cannot utilise the remedies found in the FHL. One can imagine the situation where SKF deems that it is a trade secret, even after being sold, and even if it is easy to reverse engineer the sensor. The only way to test if this is true or not is to bring the matter before a court that then has to decide if it is a trade secret according to FHL. Theoretically this can be done, but it depends on the power SKF has in the business arena. In a situation where the buyer has a low degree – or none – of power in the business arena, e.g. is a start-up or a SME, SKF could more easily force upon that this is a trade secret according to FHL and that the remedies according to that law will be enforced. In a scenario where the buyer has equal – or more – power it is identified as a risk since that actor most likely has the resources and will to take legal actions. However, what is important to mention is that the business arena described is restricted to Sweden, since the FHL is Swedish national law. Therefore it is possible that the sensor might not be acknowledged as a trade secret in for example Germany or France, since this is a different area business arena and the same law is not applied there.

9.2 EU Analysis of Article 2

The following will analyse whether or not the sensor will be deemed as a trade secret according to the Directive. Given that it is only a proposal, and therefore lacks guiding case law and doctrine, the analysis is rather short and has by nature a speculative character.

9.2.1 Information

With a teleological interpretation as a starting point, meaning that the term should be given a wide scope, the sensor fulfils this criterion. The sensor is furthermore considered as explicit knowledge since it is possible to transfer it or write it down in a manual for example. Regarding the question that the Directive does not cover trivial information, whereas it may be covered by the FHL, it is identified that the sensor most likely is not of trivial character that is addressed in the Directive. An overall assessment shows therefore that the sensor fulfils the "information" criterion.

9.2.2 Secrecy

Given that the secrecy prerequisite has a relative meaning just as it has in Sweden, shows that the sensor might be known for several persons without losing its characteristics as a trade secret. As was identified under the FHL analysis, it is possible to maintain the secret character of the sensor. It is furthermore identified that article 2, section 1 (a) states that "is secret in the sense that it is not, as a *body* or in the *precise configuration* and *assembly of its components"* (author's emphasis), meaning that there is no doubt that the sensor as a body, or its assembly of components, can be of trade secret character. This wording does not exist in the FHL and it is identified as a good contribution for knowledge that is manifested physically, since it removes any doubts whether or not the sensor or its assembly can be of trade secret character. Regarding the question what happens when the trade secret is sold, i.e. put on the market, one can only speculate. The most likely speculation is that if sold and easily accessible the trade secret loses its secret character. Just as in the Swedish regulation, a business model focusing on licensing out the sensor to certain, but not all customers, instead of selling it, is more preferable since it is easier to maintain control of the circle.

9.2.3 Commercial Value

The sensor grants SKF a certain advantage against its competitors. The advantage is identified as both a direct and indirect advantage since it improves the product and it is of great value for SKF's competitors. Therefore, if the competitors would get access to the information SKF will suffer damage. It is therefore identified that the commercial value prerequisite is fulfilled.

9.2.4 Activity

The sensor is either mounted on machines or embedded within the bearings that belong to the customer and therefore the sensor will be in the customer's premises. This means that the circumstances are such that in order for it to be deemed that reasonable steps have been taken, the sensor needs to be protected relatively carefully. Since there is no case law or further clarification of the prerequisite, it is hard to analyse what is deemed as reasonable steps. It is most likely not enough

to just mark the sensor as "classified information" given that it is in the customer's premises and of great value to SKF. Therefore more steps will have to be utilised.

9.2.5 Conclusion

Since the Directive is still not in force and therefore lacks further clarification, a conclusion merely becomes a prediction. However, as identified in section 3.2, because of the influences from Swedish law some predictions are deemed as more likely than other. The Directive has, in comparison to Swedish law, some advantages when it comes to analysing whether or not embedded knowledge is covered. For example the Directive clearly states that physical knowledge, in its assembly, components, or as a body can be of trade secret character. The Directive has furthermore an advantage by stating that different steps needs to be taken in order for the directive to cover the knowledge, making it easier for traders to apply adequate protective measures. An overall assessment shows that the Directive will most likely identify the sensor as a trade secret.

Following Petrusson's and Heiden's theory on assets, property, and capital, the introduction of the Directive will make it easier to propertise the trade secret since the Directive will develop the system of ownership rights of the trade secrets by making it more homogenous throughout the European Union. This is one step towards making it possible to capitalise on trade secrets by dynamically using them.

Regarding the three arenas, the lack of an administrative arena, means that anyone can claim their knowledge as a trade secret without applying for it anywhere. This claim can then be tested in the judicial arena where the court settles whether or not the knowledge falls within the scope of the Directive. It is identified that the business arena is of even more crucial importance, since a strong position in this arena means that it will be easier to claim the knowledge as a trade secret and property. A smaller enterprise can claim it in the business arena, however, with its weak market power will make this harder. It could therefore be said that small enterprises are only left to claim it in the judicial arena, which is a costly operation. Therefore a company such as SKF benefits greatly from the Directive.

9.3 Analysis of Scope of Protection

The following – as stated in the introduction – risks are identified as the most imminent: dismantling the sensor, acquiring information through NDT, transferring it, steal it, and bankruptcy situations. This section will analyse whether or not these risks are covered by the FHL. In the FHL it is the four prerequisites 'acquires', 'exploits', 'discloses', and 'unwarranted' that define whether or not it is

unwarranted infringement. When it comes to the Directive it is the prerequisites 'acquisition', 'use', 'disclosure', and 'unlawful'. This analysis is done to identify whether or not these two acts offer sufficient protection in order to transact the sensor, i.e. the embedded knowledge.

9.3.1 Dismantling the Sensor

According to Fahlbeck's analysis the term acquiring implies that something new has to be added to the trader's sphere. The question is therefore if the trader, by licensing the sensor, is getting something 'new' when she dismantles a product she already had in her possession? The typical case is that the trader licenses the sensor without knowing how it looks inside and what components it is made off. With this viewpoint, that it is the knowledge inside that is the interesting aspect, it can be said that she has not added anything new to her sphere. However, one can argue that she already had the knowledge in her sphere, especially if the sensor is not protected by any measures, i.e. already by having it in her possession it should be considered that she has the knowledge as well since it is more or less readily accessible. Law or doctrine does not address this question but the author identifies that if the sensor is heavily protected, the customer does not acquire the knowledge within. By dismantling the sensor the trader will get this information and thereby adding something to her sphere. The conclusion is therefore that the prerequisite "acquires" is most likely fulfilled in such a scenario. However, the question is then whether or not this is an unwarranted acquirement?

The analysis of the term unwarranted also shows that in order to not be unwarranted is if the licensee has the consent of the licensor (SKF) or any of the other ways that are identified in the above analysis section. In this case it is the consent of SKF that is the only applicable way that can authorize an acquirement. The analysis of the unwarranted prerequisite shows that consent can be given explicitly or implicitly. If the trader understood – according to the circumstances – that she had the consent to do something, she could do it. An e contrario interpretation of this gives that a trader could implicitly understand that she did not have the consent to do something with the sensor, i.e. there is an implicitly understood restriction to dismantle the sensor. Implicit agreements depend on many circumstances but one can imagine the case where the buying trader purchases the sensor and that it is heavily protected. i.e. it has locks or other protective measures making it hard to dismantle. Can this be a circumstance that implies that the trader should have implicitly understood that she could not dismantle the sensor? Much point to that it should be understood by the trader that she did not have the consent to dismantle the sensor, since it is rather obvious that she should not dismantle the sensor given the protective measures. However, since it depends on the

circumstances in each case, it can never be said for sure that this is the case. But by highlighting this question it is identified that there is some uncertainty when it comes to unwarranted acquisitions.

In the case where the sensor is sold to the trader, one has to rely on the implicitly understood agreements. The reason for this is that no other agreements are entered other than the ownership right for the sensor is transferred for payment. This is a risk that is identified with a business model focusing on selling the sensor. One way to ensure that it is an unwarranted acquisition is to rather license out the sensor than selling it. If the licensing agreements address the ownership and usage limitations, it is much easier to establish whether or not dismantling of the sensor is unwarranted or not. The reason for this is when the licensee only has licensing rights to the sensor, the presumption is that she cannot do anything with the sensor without the consent of the licensor or something that has explicitly been agreed upon. Therefore the licensing agreement has to address the question what the licensee can do or not do with the sensor. However, this shows that it is not the FHL that gives the immediate protection, but rather the business model and the agreements that are attached to it. Although the FHL might be applicable even if this has not been regulated through an agreement, i.e. the licensee should have implicitly understood that she could not dismantle the sensor because of the licensing agreements and the measures protecting it, it is identified that it is easier to establish whether or not something is unwarranted or not when agreed upon through contracts.

Dismantling the sensor, or trying to get access to the information within in it in any other way, is regulated by the Directive in article 3 paragraph 2. As mentioned in section 8.4 and the appendix, unauthorized access of an object from which the trade secret can be deduced, and that is lawfully under the control of the trade secret holder, is unlawful when carried out intentionally or with gross negligence and without the consent of the trade secret holder. The same reasoning as in the paragraph above can be made here. Much point to that when the sensor is sold, the trader has the consent to access the information within the sensor since ownership rights have been transferred. The trader can reverse engineer the product and as a first step dismantling it in order to acquire the information legally. The question can be asked whether or not it should implicitly be understood that they did not have the consent to dismantle the sensor but this is – as identified in the paragraph above – as very unpredictable. A difference from the FHL is the wording "and that is lawfully under the control of the trade secret holder". The question here becomes what is the meaning of 'under control'. In the case where the sensor is sold it could be established that SKF does not have any control, neither legal control since the ownership rights have been transferred

without any restrictions on how to use the sensor or control in the sense that they have physical control over the sensor. However, in a licensing case it is identified that they still have the ownership rights through an agreement, i.e. legally in control, and therefore much points to that this prerequisite is fulfilled even if they still do not have physical control, i.e. they have it in their possession.

9.3.2 NDT

The question is whether or not the FHL covers the situation where a customer tries to acquire the information within the sensor utilising NDT. Conducting NDT relates to the risk that the customer "acquires" the information. In order to avoid reiteration the same reasoning as made in the section above, 9.3.1, applies here. The conclusion is therefore that accessing information using NDT is identified as acquiring information. The question how much, or how accurate the information is, makes most likely no difference.

As in the section above the question comes down to whether or not the act of using NDT is unwarranted or not. Conducting a sales model implies – as mentioned before – that the customer can do whatever she wants. This is due to that there are no explicit restrictions to do so. Again it can be argued that there are implicit agreements restricting such use. When conducing a license model the starting point is that all acts, which are not explicitly or implicitly consented are illegal. Therefore, trying to use NDT in order to acquire information within the sensor will be identified as an unwarranted acquisition, which is covered by the FHL. It is however another question that it is most likely hard to establish that the customer has conducted NDT, meaning that such acts in practical cannot be covered by the FHL

Analysing this imminent risk from the protection given by the Directive gives more or less the same answer as in the section made above, 9.3.1. Therefore a more extensive evaluation will not be conducted. It is enough to establish that when the sensor is sold a NDT will most likely not be identified as an unlawful acquisition and as an unlawful acquisition when licensed out.

9.3.3 Transfer

In a situation where a trader has purchased or licensed the sensor legally, is she able to transfer the sensor without the FHL recognising it as an unwarranted infringement? Such action relates to whether or not the buyer has disclosed the information. As described in the analysis above it is established that a trade secret can be disclosed when it is transferred as an object from which the trade secret can be deduced. Therefore a transfer of the sensor can fulfil this prerequisite. Even if Fahlbeck's example analyses an employee stealing the trade secret and then giving it to a trader

willing to acquire it, some guidelines can be read from it. There are two steps: in the first step, the sensor has to be unwarrantedly transferred to a trader, and in the second step the trade secret has to be known for the acquiring trader. Yet again it boils down to whether or not this is unwarranted or not and if the trader actually accesses the secret information. As identified in the other risks, when the trader buys the sensor much point to that transferring the sensor to a third party cannot be identified as an unwarranted infringement. In a situation where the transferring trader has acquired the sensor from SKF by a licensing deal, this behaviour would most likely be identified as an unwarranted disclosure according to the FHL, since the transferring trader has not ownership rights but rather only licensing rights and therefore has no right to transfer it to a third party without the consent from SKF, i.e. she breaches the licensing agreement when transferring the sensor. Therefore, in the licensing deal the first step is most likely fulfilled.

Question is however if the second step is fulfilled. Undoubtedly the third trader acquires the sensor but does she acquire the trade secret that is protected within the sensor? This question is not addressed in case law or doctrine and therefore one can only speculate. An example with blueprints can be made. Even if the blueprints are transferred in an envelope they surely have to be identified as transferred even if the trade secret, at first glance, cannot be seen. The trader can simply open the envelope in order to access the information. In the case with the sensor it is the plastic cask that conceals the trade secret within it and it is undoubtedly harder to open than an envelope. Given the precision that can be achieved by modern machines today, it is easy to open up a sensor that is only protected by a plastic cask. If the sensor on the other hand is heavily protected by different measures, it can be argued that the acquiring trader per se does not know the trade secret and therefore remedies according to the FHL cannot be demanded. However, if the acquiring trader would somehow, against the odds, be able to access the information, it will be identified as an unwarranted disclosure since the second step of Fahlbeck's analysis is fulfilled. This speculation follows the same reasoning that the SOU 1983:52 and Levin has when stating that something that is not easily accessible for a person skilled in the art can maintain its secret character even when it is put on the market. The conclusion is therefore that in a situation where the sensor licensed to a trader, the FHL might be utilised to remedy an act where the sensor is unwarrantedly transferred to another trader.

A relevant question is whether or not the sensor loses its characteristic as a trade secret when it is disclosed after being transferred? As the analysis of the applicable law states above, several traders can know of the secret without it losing its characteristics. Fahlbeck mentions that when the

transfer is unwarranted the answer whether or not it loses it characteristics depends on the circumstances.[130] If it is clear that the information has been disclosed to a certain trader, which can be identified, and this trader realised, or should at least realise, i.e. is in bad faith, that it is secret information she has been given, the information ought to maintain its character as a trader secret. An e contrario analysis shows that if the trader did not know she was given a trade secret, or it cannot be identified which trader was given the information, the sensor will lose its characteristics since the acquiring trader was in good faith and this is always considered as a warranted infringement. The reasons for this are that it is possible to acquire trade secrets in good faith, meaning that the trader is not responsible for any infringements. As mentioned by Fahlbeck, this applies to all traders if the trade secret has been transferred in several steps, i.e. all the traders need to be in bad faith.

The directive has a straightforward approach to whether or not transfer to a third party could be identified as an unwarranted disclosure or use. By identifying a person who meets any of the three conditions, the person has committed an unlawful use or disclosure of a trade secret. The first condition states that the person has acquired the trade secret unlawfully. In the case where the trade secret is either sold or licensed out to a trader it is – as mentioned above – identified that the trader has lawfully acquired the sensor. Therefore the first condition is not fulfilled. The second condition states that it is a breach or inducement to breach a confidentiality agreement or any other duty to maintain secrecy. In the case where the sensor is sold it most likely means that there is no breach since there is no confidentiality agreement. However, the wording "or any other duty to maintain secrecy" could imply that if the sensor is heavily protected, the trader should understand that she has a duty to maintain the secrecy. However, protecting the sensor with different non-legal tools, such as stamps or locks can be used as a strategy to leverage that this condition is fulfilled in the case where one sells the trade secret. In the case where SKF licenses out the sensor, the party who transfers the sensor to a third party, or steals, the situation is different. Licensing agreements usually contain confidentiality agreements and if such exists this condition is fulfilled. The third condition states that if the person is in breach of a contractual or any other duty to limit the use of the trade secret it should be deemed as unlawful use. When the sensor is sold the most likely situation is – as mentioned – that there is no explicit contracts that are entered. The wording that states: "or any other duty to limit the use of the trade secret" resembles to the wording used in the second condition. The wording has the character of a general clause that could be used if any of the

[130] Fahlbeck (2013), p. 322.

other two conditions are failed to fulfil. In the licensing situation this condition will most likely be fulfilled, but as mentioned, it is most likely already covered by the second condition.

The overall assessment shows that in the case where the sensor is sold it will most likely not be considered as an unwarranted infringement according to both FHL and the Directive. The situation where the sensor is licensed out is on the other hand most likely covered if confidentiality agreements are entered.

9.3.4 Stealing

A scenario where the sensor is stolen relates to different situations depending on what the actor who has stolen the sensor does. The most imminent risk is that an employee steals the sensor. Such action can be identified as an unwarranted acquisition of the trade secret. There is no need to identify whether or not the employee has learned the information since it is not a requirement that the employee takes part of the information, the employee can for example be passive and only "steal" the information in order to transfer it to a third party as is identified in the analysis. If the employee transfers the knowledge to a third party, it is most likely identified as an unwarranted disclosure of the trade secret, see the above section for a more extensive investigation. One can also imagine the scenario where a trader conducts business espionage in order to gain the information. Such action is also identified as an unwarranted acquisition and is especially addressed in article 3 of the FHL.

The directive is yet again more straightforward compared to the FHL. Article 3 section 2 (b) addresses this situation by stating that it should be considered as unlawful acquisition when someone has, without consent, acquired the information through theft. Therefore a situation where an employee or a competing trader steals their information is without a doubt covered by the Directive.

9.3.5 Bankruptcy

As mentioned under section 10.1.4, the official trustee is responsible for reimbursing the creditors when a company enters into bankruptcy. The trustee must many times sell everything that is in the bankruptcy estate in order to be able to reimburse the creditors. It is therefore identified that the trustee, as bought by the trader who has entered into bankruptcy, will most likely sell the sensor, to a third party. However, the official trustee also has the possibility to enter into the agreements that were entered by the trader and therefore keep fulfilling them. The question is if the FHL or the Directive covers this situation? The situation where the trustee sells the sensor in order to reimburse the creditors will be analysed first. Secondly the situation where the trustee enters the agreement will be analysed.

The situation where the trustee sells the sensor to a third party relates to an unwarranted disclosure. As mentioned there are two steps to consider, 1) the sensor needs to be unwarrantedly transferred to a trader, and 2), it has to be known for the acquiring trader. Whether or not it is unwarranted according to the FHL depends if the trader has consent or not. In the situation where the sensor is sold, the trustee can transfer it to a third party since any action is warranted if no implicit agreements have been entered. This applies even if it is the trustee and not the initial trader who transfers the sensor since the trustee is to transform all the property that belongs to the bankrupt trader, into 'liquid assets'.[131] In the situation where the sensor has been licensed out the situation is different since the bankrupt trader does not own the sensor. Much points to that this situation is solved with the same reasoning that was mentioned above under the risk "transferring the sensor", i.e. the first and the second step is most likely fulfilled since the trustee did not own the sensor and the acquiring third party knows about the secret if it is not so heavily protected that a person skilled in the art can easily acquire it. Therefore this can be identified as an unwarranted disclosure. However, yet again, this depends on that there is a licensing agreement and not that the FHL covers it per se.

It is considered a general legal principle that the bankruptcy estate has the possibility to enter into the agreements of the bankrupt company, or not if that is what the bankruptcy estate wishes to.[132] Therefore an outcome could be that the trustee enters into the licensing agreement that was made with the now bankrupt trader. This does not have to mean that it is a bad thing for the licensor but it is established that the FHL offers no protection for this scenario. This situation needs to be solved by using other tools.

Regarding the Directive, article 3 paragraph 3, the outcome is most likely the same in the situation when the sensor has been sold to the now bankrupt trader. Regarding the scenario where the sensor is licensed out, article 3 paragraph 3 is the most relevant one. The second condition is the most relevant one but if this might not be fulfilled the third condition, which has the character of a general clause, is most likely fulfilled.

9.3.6 Conclusion

Applying the theory of dynamic use of intellectual property, the question is whether or not FHL allows for such use of the knowledge within the sensor. As it is established that FHL most likely acknowledges the knowledge as a trade secret, according to the legal definition, it is theoretically

[131] Folkesson, Enar, Företaget i Ekonomisk Kris, 7th Edition, Thomson Fakta, 2007, p. 125.
[132] Folkesson (2007), p. 129.

possible to use it dynamically. However, practically the protection given by FHL, as stated by Levin as well, is often times "toothless" (author's translation).[133] This analysis shows that the control given by FHL is low if not protected by other legal tools, such as agreements. An example is that anyone can reverse engineer the product if they have bought the sensor legally. Therefore it is identified as almost impossible to sell the product and maintain the secret character. There is an option to rely on that the trade secret is so hard to access that a person skilled in the art cannot easily do this. When so, the trade secret maintains its secret character. This is however, as mentioned, very unpredictable and not advised. However, safeguarding the sensor with different measures is still interesting, but not as a sole measure. The business model that is identified as best suitable is the licensing model. This business model allows it too much easier show that any infringement is unwarranted. The reason for this is that one can then contractually agree upon what should be an unwarranted infringement or not. It can however not be mentioned too many times that the contractual agreements are separated from FHL and acts as a way to easier utilise the FHL.

As mentioned under the theory section, having control over an identified asset is key in order to make it valuable. If the knowledge is seen as public it is hard to persuade a trader to buy it. Above it was established that the sensor can be acknowledged as a trade secret according to the definition of the FHL and the Directive and that this allows for claiming the knowledge within the sensor as property. However, one can argue whether or not this is a strong property claim. Generally a claim derived from Swedish law ought to be strong, in the sense that it grants the proprietor or owner a good control position. However, this depends mainly on the system of ownership rights surrounding that claim. The analysis shows that it is rather easy to claim something as a trade secret, which have to be a factor that suggests that the claim is not strong. Furthermore, lack of an administrative arena also suggests that the strength of the property claim is not strong. A third factor is that the trade secret claim grants no exclusivity for the knowledge. A fourth factor is the volatile nature of trade secrets, as shown in the analysis. A comparison can be made towards the patent and the system surrounding patents. The patent system gives the proprietor or owner a strong claim to the knowledge patented. The reasons for this is that there is well established ownership rights in the form of a well developed administrative arena that grants exclusivity which is upheld by more or less all business actors. The conclusion is therefore made that the property claim from a trade secret is identified as a weak property claim.

[133] Levin (1996), p. 376.

The analysis shows that the protection from the two legal acts is not impregnable. This implies that even if SKF can claim that the sensor is a trade secret, it would not matter since it is hard to capitalise on it. In order to dynamically use trade secrets the level of control needs to be at a certain level. It is hard to establish where this level is but the author argues that with only the FHL and the Directive as protection the level of control is not sufficient. Capitalisation can still occur, but in order to create a foundation for a platform, the FHL and the Directive is not enough. However, applying the theory of the three arenas to the conclusion that the FHL and the Directive offers poor protection for transacting knowledge, can give other results. The argumentation for this is that an actor with power in the business arena has a greater chance to uphold the protection compared to an actor with no or less power within the business arena. For example, if SKF transacts knowledge to an actor who has little or no power within the business arena compared to SKF and SKF only relies on the protection offered by the FHL and the Directive, this protection will be identified as stronger than the protection when both parties have equal strength within the arena. The reason for this is that the actor with no or less power is more likely to depend on trade with an actor with influence in the business arena. That actor is therefore less prone to infringe the trade secret since it will damage the business relationship with the actor who has power in the business arena. Therefore the protection offered by the FHL and the Directive is relative when applying the theory of the three arenas. Depending on the circumstances the protection can be identified as more or less protective, i.e. the FHL and the Directive offers different amounts of control depending on the power within the business arena.

10 Openly Available Knowledge – Analysis of FHL and the Directive

In the following an analysis will be performed whether the manual, both digital and analogue, and the information contained therein can be claimed as property, i.e. trade secrets, in the business arena according to the FHL and the Directive. Petrusson argues that describing information as trade secrets is a claiming process and if the claims are accepted in the business arena, the holder has a trade secret that can be seen as her intellectual property.[134] Describing information as trade secrets implies that the legal prerequisites for knowledge to be seen as trade secrets must be fulfilled for both FHL and the Directive. Finally it will be analysed what protection is granted by the both legal acts.

[134] Petrusson (2004), p. 115.

10.1 FHL Analysis of Article 1

In the following will be analysed if the knowledge in the manual is considered as a trade secret according to the FHL. The structure for the analysis is the one used above when presenting the legal background, i.e. the different prerequisites and their respective sub criteria.

10.1.1 Information Concerning the Business or Industrial Relations of a Trader

10.1.1.1 Information

The propositionen mentioned above gives that the information criteria should have a wide meaning and that it can be of many different sorts as long as the information is possible to document. Furthermore praxis gives that there should be no quality requirements on the information, implying that even if the information presented in the manual is of a simple nature it should still be deemed as information in a legal sense. Of the examples presented above are for instance seen construction drawings, which without doubt will be present in the manual when showing how to mount the bearing. The manual also contains information of other character as well, but as the example list is not exhaustive, that there should be no quality requirements on the information and due to the wide meaning of information, the conclusion must be that the other information is considered information in a legal sense as well. The criterion that the information should be possible to document and not only reside in the minds of humans is fulfilled in the case of the manual as it is written down, i.e. documented. The fact that the manual might be of a digital character will not affect the conclusion since it is explicitly stated in the propositionen that the information may be stored on a computer memory.[135] In summary the information contained in the manual is considered information from a FHL perspective, regardless if the manual is digital or analogue.

10.1.1.2 Business or Industrial Relations

The information must concern the business or industrial relations of a trader. As has been stated above, this criterion should be interpreted as that the information must be linked to a company and the economic activities within the company, and not be generally known. As the manual covers information of how to mount the bearing it must be seen as linked to both the economic and industrial activities of the company, as the production of bearings is the core activity of the company. The company also has operations that work solely with mounting bearings, therefore, in relation to that business unit within the company, the link is quite strong. The existence of this business unit indicates that the information is not generally known, otherwise the customers could,

[135] 1987/88:155, p. 65.

and likely would, do the mounting themselves or contract a third party to mount them. The business case would at least not be as favourable if the information used by the mounting service is generally known to anyone who might want to compete with a similar service. In summary the criterion that the information must concern the business or industrial relations of a trader is fulfilled.

10.1.1.3 Trader

The third criterion that the holder of the trade secret should be considered a trader is a generous criterion. A trader is any physical or legal person that in a professional manner conducts business, regardless of whether the business aims at making a profit.[136] As the company in this case is a multinational legal person that has profits of billions of SEK, and is considered to be in the forefront of the technical advances within the area, the company is without doubt considered a trader from an FHL perspective.

10.1.2 Secrecy

10.1.2.1 The Time Factor

The time factor implies that even if the manual was developed several years ago, it will still be considered as a trade secret if the other prerequisites are fulfilled. This applies even if SKF would make a new version of the manual in the future, following the case NJA 1999 s. 469, as have been accounted for under section 8.1.2.1

10.1.2.2 Circle of People

For the information to be considered and protected as trade secrets there is a requirement for the trader to keep the information secret, however, this prerequisite is not absolute in the meaning that no one may know the information. There are no limitations on how many may know the information, there is however a requirement for the circle of people that knows the information to be closed and identified. It is also noted above that as long as the information is only distributed to the people that need the trade secret to conduct their work, then it should be considered as kept secret. For the time before the manual is transferred to the customer the information is most likely considered secret as long as the information is known only by the persons who need the information to do their work and the ones writing the manual, which would then be considered as a closed and identified circle. Once transferred to the customer it can continuously be considered secret if the identified and closed requirement is fulfilled. If the circle of people that is allowed to read the manual are the people that are going to use it when mounting the bearings, then that circle would

[136] 1987/88:155, p. 34; Wainikka (2010), pp. 39-30.

most likely be considered as "identified and closed" and the information considered secret as long as the information is kept within that circle of people. If the information is available outside the circle of people that need it to mount the bearings the circle of people might not be considered "identified and closed", which is something that would have to be settled by a court of law in the judicial arena. As the manual is custom made, and not for available to anyone who might be interested in it, it will be possible to establish an identified and closed circle since SKF can choose the customers. If the manual is widely sold or licensed, as identified in the SOU 1983:52, it is impossible to have an identified and closed circle and the secrecy prerequisite is not fulfilled. It is however unclear where the line should be drawn more specifically for the circle to remain identified and closed why caution should be exercised when transferring trade secrets to a third party, as well as when keeping them secret in-house.

10.1.2.3 The Activity Criterion

There is also an activity criterion for the information to be considered secret, which implies that the trader shall have the intention to keep the information within a limited circle of people and has taken some sort of measure to realise this ambition. An e contrario interpretation gives that if the information is secret just by luck, without the trader having any intention of keeping it secret and not have taken any measures to ensure the secrecy, then the activity criteria is not fulfilled. It is however very difficult for another party to prove that the activity criteria has not been fulfilled, why the risk is most likely low if the information is secret by luck. The case T 8471/99 states that if the objective criteria is not fulfilled, i.e. no measures have been taken as to ensure the that the information is kept within a certain circle of people, it might be 'healed' if it is customary within a specific line of business to keep such information secret, implying that the trader that receives the information should have understood that he is not allowed to disclose the information. In the case of the manual it will most likely be considered as trade secrets before distributing it to the customer, as long as the trader has in some way expressed to the employees that they must not tell the information contained within the manual to any third party, for instance by having a secrecy clause in their employment agreement. After transacting the manual with the customer there is still no difficulty to ensure that the activity criteria is fulfilled by having the customer sign an NDA, or similar. If no such measure have been taken it presents difficulties for the trader to prove that, if so is the case, it is customary in that line of business to keep the information secret. However, as the activity criterion is low it is rather simple to fulfil it why some measures should always be taken to ensure that it is fulfilled.

10.1.3 Damage

9.1.3.1 Disclosure Likely to Cause Damage

The third prerequisite for information to be considered as trade secrets is whether it is likely to cause the trader damage from a competition point of view, if the information is disclosed. This damage does not have to be only economical and there is neither any requirement that any damage has actually occurred, but rather if it is a situation which typically would cause damage for the trader. As there is no requirement that any damage has actually occurred it is rather simple to affirm that the situation of the manual is likely to cause damage. There are separate business units within SKF that work with mounting bearings, which use the information that is documented in the manual. Sharing this with a third party is therefore likely to cause damage to that particular business unit if the manual is disclosed, either by the receiving party or an employee of SKF.

10.1.3.2 For Which Trader

There is also a need to establish for which trader the damage has occurred, or is likely to occur. It is rather clear that it is SKF that would suffer the damage, as it is their trade secrets that the manual is comprised of. The receiving party may also be damaged if that knowledge presented her with a good competitive advantage or similar. Such damage is however more insecure and depending on the specific case why the only damage that would be for sure, if the trade secrets were disclosed, would be for SKF

10.1.3.3 Damage From Competition Point of View

Finally the disclosure has to actually damage the possibility to compete. As has been mentioned SKF has business units that work solely with mounting bearings, and when doing so they utilise the knowledge within the manual. If this information would come into the hands of other customers than the one who received it, or worse, if it got into the hands of a competing firm, it would without doubt damage the ability for SKF to compete within this area. The major advantage SKF has over the competitors is that SKF knows exactly how the SKF manufactured bearings should be mounted, if this information is instead freely available the competitive advantage is diminished.

10.1.4 Conclusion

As a general conclusion the manual, both digital and analogue, fulfils all the prerequisites according to the FHL for being claimed as a trade secret in the business arena, which is where it has to be claimed since there is no administrative arena. In other words, there is no doubt that the manual may be claimed as property using FHL.

Due to SKF's size and market power the manual will benefit from stronger protection than that of a small company, since SKF can leverage their power in the business arena, something that a small company cannot do the same way.

It should also be recognised that if the manual is widely sold or licensed to anyone who might be interested in it, it will to all certainty not be considered as a trade secret, but rather publicly available knowledge. Therefore it is advisable to hand pick a few customers instead of widely distributing the manual.

Something highly important in the case of the manual is what happens when the manual contains information that is both generally known and information that is claimed as trade secrets. In such a case, will the manual as a whole be protected as a trade secret or not? It comes down to if the manual as such can be claimed as a trade secret or if only the information within the manual can be trade secrets. A parallel can be drawn to customer lists that comprise public information, namely people's names and addresses, but are still considered trade secrets. The names as such are public but the fact that those specific people are customers to a company is a trade secret. This implies that if you have public information but add another dimension of information to it, and use it in a specific context, then it can still be considered trade secrets. The secret dimension that they are customers, of the information is then very small compared to the public dimension, their name and addresses, of the information. The conclusion must therefore be that even if the majority of the information is publicly available the entirety can be claimed as a trade secret. If the same reasoning is applied to the manual it will most likely be possible to claim as a trade secret even though some of the information contained within is publicly available. A teleological interpretation of the FHL gives the same outcome, since the protection otherwise would be illusory. If it would not be like this, a trader would lose the protection over a document containing highly important information if a single aspect were to become publicly known. The conclusion is therefore that even if some information in the manual is publicly available the manual as such will be possible to claim as a trade secret and property of SKF.

10.2 EU Analysis of Article 2

In the following will be analysed whether the information in the manual, both digital and analogue, will be considered as trade secrets according to the Directive. The four prerequisites that are needed to be fulfilled in order for the manual to be seen as a trade secret are information, secrecy, commercial value, and activity, which will be analysed in the following.

10.2.1 Information

Above has been stated that the term information must be given a wide meaning to give an effective protection for trade secrets. The directive itself also says that the "definition should therefore be constructed as to cover business information, technological information and know-how".[137] However, neither tacit nor trivial information should be covered. The manual contains technological information as well as know-how on how to install the bearings. As the manual is written down the information is not tacit, since such information is impossible to document. The information is not trivial either as it is obviously of great importance when installing bearings in wind power stations. Given the wide interpretation of the term information, the information in the manual must as a conclusion be considered as information in the meaning of the Directive.

10.2.2 Secrecy

As the secrecy requirement is of a relative nature, this implies that the information in the manual might be known outside of SKF, under certain circumstances at least. The important distinction is if the information is generally known within the circle that normally deals with this information or is readily accessible to them. Before the manual is transferred to the customer it will almost certainly be considered secret, and after the transaction as well, since transferring the manual to one company will not imply that it is generally known in the relevant circle. It is however unclear where the line should be drawn for when the information would be considered as generally known, is the majority of cases it would definitely require more persons to be aware of the information that in just one company. The criteria that the information should be readily accessible to people within the relevant circle cannot be interpreted so that just because one company is allowed to buy or license the information from SKF it is considered readily accessible as it is possible to get access to the information this way. If that were the case it would imply that transfer of trade secrets would not be possible, since they would no longer be trade secrets. It should also be noted that if the manual is widely distributed it will be very difficult for the manual not to become generally known in the relevant circle and no longer be considered as a trade secret, why this is not advisable.

10.2.3 Commercial Value

That the information within the manual has a commercial value is a conclusion that is easy to arrive to. To be able to install bearings in wind power stations the information in the manual is required since installing the bearings is very difficult and impossible to do without the information within the

[137] European Commission Proposal (2013), pp.12 - 13.

manual. The party that has access to this information has a competitive advantage as that party may then install the bearings. A competitive advantage like this is highly valuable, which is also shown when SKF has a business unit that works with installing bearings in situations like this. If SKF can base parts of an entire business unit on the information within the manual, and similar information relating to other bearings, the information is undoubtedly valuable.

10.2.4 Activity

What should be considered reasonable steps to keep the information secret is dependent on the circumstances in the specific case. If the information is transacted outside the company, the activity level, i.e. the reasonable steps to keep it secret, must be higher as the trade secrets are more vulnerable once transferred, especially if widely transferred. The same applied if the information is highly valuable, the required activity level is most likely higher than if the information is not very valuable. What in the individual case should be enough is unclear, but the fact that the requirements are relative, sends a clear signal to the trade secret holder to add more protection to ensure that the activity criterion is met. In the case of the manual there is probably a need to use both contractual protections, such as secrecy clauses, as well as marking the manual with "secrecy" and probably other protective measures as well to be on the safe side.

10.2.5 Conclusion

First and foremost there is a need to recognise that the Directive has not yet entered into force, why the analysis of it has a big proportion of prediction. With this in mind, the manual, both digital and analogue, will as a conclusion be considered a trade secret according to the Directive for the time before it is transferred to a third party, as long as it is kept secret. Just as under FHL the fact that the manual might comprise both secret and public information should not affect the trade secret status of the manual as a whole as the protection would then be illusory. One criterion may present issues is the activity criterion, the other ones are rather straight forward that they are fulfilled. When the manual is being transferred on the other hand, there is a need to apply more protective measures to ensure the secrecy of the manual. Where the line should be drawn as to when the activity criterion should be considered met is unclear, and is most likely decided in the individual case. It does however show that when transferring trade secrets a trader should be cautious and rather use too much protection than too little. Utilising few strong protective measures or many less strong ones may for instance do this.

Lacking an administrative arena a trade secret needs to be claimed in the business arena instead, and then later upheld in the judicial arena if needed. Just as in relation to FHL above there is

no doubt that the manual may be claimed as a trade secret and thereby property according to the Directive.

It is clear that since a trade secret is claimed in the business arena, the size of the company claiming the trade secret, and their inherent market power, will affect the protection of the trade secret, as a big company like SKF may leverage its market power into better protection. It could however also lead to higher requirements for protective measures, as the activity criterion is dependent on the circumstances in the specific case.

Given Petrusson's and Heiden's theory the proposed Directive will make it easier to capitalise on trade secrets than before due to the harmonisation of the rules concerning trade secrets. Claiming a trade secret as property in the business arena will be made easier since all EU countries will have the same prerequisites for doing so, and protecting it in the judicial arena will also be easier due to the harmonised legislation. As a general conclusion the directive as such will therefore facilitate capitalisation of the trade secret by dynamic commercial transactions.

10.3 Analysis of Scope of Protection

It is established that the manual, both digital and analogue, is considered as a trade secret according to both the FHL and the Directive. The next step is to establish what protection is granted by the FHL and the Directive. Under the FHL only unwarranted uses are prohibited and under the Directive only unlawful uses are prohibited, what this implies has been addressed above. The question is if any of the imminent risks mentioned above in relation to transferring a manual to a customer are covered by either the FHL, the Directive, or by both. For this to be the case the risks below need to be an acquisition, exploitation or disclosure according to FHL or the Directive, and on top of this unwarranted or unauthorised. If this is the case will be analysed in the following where each individual risk will be reviewed after first addressing some aspects that are applicable in all cases. The analysis will be carried out as if no contractual obligations are entered into between the parties to better show what protection is granted by FHL and the Directive and which actions might trigger sanctions, mainly in terms of damages, by FHL and the Directive.

10.3.1 Good or Bad Faith

According to article 2 paragraph 3 FHL it is possible for someone to acquire a trade secret in good faith, implying that no attack on the trade secret in terms of exploitation or disclosure can be seen as unwarranted. If a trade secret is acquired by someone in good faith she can therefore do whatever she like with it, since she was not aware that it was a trade secret. As is stated above, if the trade

secret has passed several parties there is a requirement that not only the last party in the line of events is in bad faith, but also all parties before. This is therefore a potent risk when transferring trade secrets, however, Tonell indicates that it might be enough for bad faith to have confidentiality provisions in the agreement between the two first parties.[138] To be on the safe side parties should in an agreement explicitly state that the manual is a trade secret and use confidentiality provisions. Another way to ensure bad faith for a customer would be to mark the manual with 'Confidential' or 'Trade secret of SKF'.

10.3.2 The Acquisition

All risks except "Too Much Information" relate to that the manual has been transferred to the customer at some stage and then there are risks in relation to this. In all these cases the customer has acquired the manual, when transferring the manual analogously or digitally, according to both the FHL and the Directive. The customer did not have the manual in her possession before and now has, which implies an acquisition of the manual. The propositionen states that a trade secret may be stored on a computer memory why transferring the manual as a PDF will be seen as an acquisition by the customer as the manual is always stored on the hard drive of the computer or similar electronic device.[139] The Directive has most likely the same standpoint, though not explicitly. However, if a solution for accessing a digital manual is used where the customer only accesses the manual via a web-based data room or similar, where the manual is not stored locally on a computer but on a remote server, can the manual be considered to be acquired by the customer?

When the manual is downloaded to the Random Access Memory (RAM) of the computer when accessing the manual via a web page, for as long as the web page is open. RAM is a type of computer memory that can be accessed randomly, and every time you start a program it gets loaded into the RAM, which allows for faster access than running the program straight from the hard drive.[140] When the web page is closed the memory will be cleared, the copy of the manual in the RAM is a temporary one.[141]

However, as long as the computer has not been turned off and then on again, there is a possibility that temporary files of the manual might be saved on the computer. These files might in

---

[138] Tonell (2012), p. 34.
[139] 1987/88:155, p. 65.
[140] Source: "RAM" retrieved 24/04/2014 from: http://www.techterms.com/definition/ram, "RAM - Random Access Memory" retrieved 24/04/2014 from: http://www.webopedia.com/TERM/R/RAM.html.
[141] Source: "How to Clear Computer RAM Memory" retrieved 24/04/2014 from: http://www.ehow.com/how_5054182_clear-computer-ram-memory.html.

turn be possible to access by someone with enough computer skills, however when the computer is turned off any such files are deleted for certain.

A relevant question in relation to this is whether or not the customer needs to take part of the information. Fahlbeck states that the "the word acquire does not imply that acquirer takes part of the information" (author's translation) meaning that acquirer can be a passive middle hand and that the information is considered acquired already when customer has the possibility to take part of the information.[142] A trade secret is therefore considered possessed already when a customer has the possibility to access it, regardless of factual possibility to access it. For instance, if accessing the information in the RAM or the temporary files requires special competence, this will not affect the possession. I.e. in this case, when the information is in the RAM or is available as a temporary file the customer has acquired it.

When the customer accesses the manual, she might only view a certain part of it. In that case the most likely conclusion is that at least parts of the manual, what is viewed on the screen, is saved in the RAM. This would then be seen as in the customer's possession and have been acquired. Would this be enough for the manual as a whole to be possessed, and thereby acquired, by the customer? As the customer has access to the whole manual and can freely choose which part of it to view, then the most reasonable conclusion must be that even if only a part of the manual is saved in the RAM during a specific time period it must likely be seen as the whole manual is acquired by the customer. The conclusion should reasonably not differ between FHL and the Directive.

Using a web-based data room solution that downloads either parts of or the entire manual to the RAM will therefore imply that every time the manual is accessed it will be acquired by the customer, and every time the web page is closed the customer will get rid of the manual as long as no temporary files are saved. It might however be the case that the manual is not saved to the RAM when accessing it, though highly unlikely.

If the computer, or similar device, which is used for accessing the manual through the data room is not belonging to the customer but is leased from SKF, does that affect the conclusion? The reasoning for that an acquisition had occurred above was that temporary files were saved on the computer belonging to the customer. If the computer does not belong to the customer, does that imply that the customer has not acquired the manual when accessing it?

[142] Fahlbeck (2013), p. 255

Fahlbeck states that every type of acquisition of the information implies an acquisition in a legal sense.[143] This means that the acquisition does not need to be of a physical or virtual carrier, which is also discussed below in relation to 'Learning the Information'. A person can acquire information by learning it as well as acquiring the carrier of the information. When the manual is accessed on the customer's computer it will be considered as an acquisition since the customer then has control over the information, at least temporarily. If the computer belongs to SKF instead, it can be questioned whether the customer has control over the information or not. It depends on whether the customer the customer can exercise control over the information, which in turn depends on how the device has been set up and programmed. It is therefore difficult to arrive at a definite conclusion and that for it to be an acquisition for certain when using a data room and SKFs electronic device, there is a need for an employee of the customer either to learn the information, or by making some sort of copy of the manual. As long as this does not happen, it is unclear whether the customer has acquired the manual according to FHL. Reasonably the Directive would be of a similar standpoint.

Utilising the solution with a data room and SKF's electronic device implies that when the customer accesses the manual, it is for certain considered as a use according to FHL and the Directive. This use is authorised by SKF and therefore the customer has not infringed. If the customer manages to access the manual after the license has been terminated and uses it then it will be unwarranted, as SKF has not consented to it.

Will the different types of identified acquisitions above, when acquired using a data room solution, the PDF solution or an analogous solution, be seen as unwarranted according to FHL or unlawful according to the Directive? As regards the FHL the acquisition of the manual as the customer has done in this case, regardless of distribution model, since SKF has consented to the acquisition, is not an unwarranted acquisition. The same applies for the Directive where article 3 specifically says that it has to be without the trade secret holder's consent to be considered an unlawful acquisition. The acquisition of the manual is therefore considered lawful according to both FHL and the Directive.

What happens if the employee learns the information is accounted for below in relation to 'Learning the Information'. The legal implications of copying the manual are accounted for below in relation to 'Keeping the Manual'.

[143] Fahbleck (2013), p. 353.

10.3.3 Selling the Manual

Above under section 11.2.1 in relation to the FHL is stated that acquiring a trade secret by reverse engineering after first lawfully purchasing the product within which the trade secret can be found is not unwarranted. It is also stated that in such a case if the customer uses or discloses the trade secret those should be considered as warranted actions. In the case of the manual there is little need for the reverse engineering to be performed to get access to the information within the manual. Read the document and the information is there. When selling the manual to a customer the customer must therefore be allowed to do whatever she wants with it. Reasonably the protection granted by the FHL must be the same regardless of how the information is packaged why the same rules should be applicable for reverse engineering both for analogous and digital products.

Most likely the same principle is applicable under the Directive, however as it is not yet implemented it is difficult to know for certain. However, it is established that the Directive has drawn inspiration from the FHL, which further supports the thesis that the same principle is applicable under the Directive as under the FHL. If this is the case it implies that the customer can do whatever she wishes with the manual, use it in-house, disclose it to anyone she wishes or sell it to a competitor of SKF under both the FHL and the Directive.

10.3.4 Licensing the Manual

As the control over the manual is lost when selling it, as has been established above, the following analysis of FHL and the Directive will focus on the case when the manual is licensed from SKF to the customer.

10.3.4.1 Too Much Information

As SKF is the party that decides how much information should be in the manual, and it is their own knowledge, having too much information is neither unwarranted according to the FHL nor unlawful according to the Directive, why this risk is limited by neither the FHL nor the Directive.

An interesting question is instead what happens if the information within the manual is limited as an attempt to address the risks associated with having too much information, for instance by letting necessary calculations be made outside of the customer's control using an external device, a web page or an interactive manual, see section 15.2. This might affect the claim of the knowledge within the manual as trade secrets, however unlikely given the generous interpretation of what is considered information by both FHL and the Directive.

If the manual and the external device are licensed to a customer it is obvious that the information that is still within the manual has been acquired. For the information that is stored

inside for instance an apparatus it is not as obvious. If the device is simply handed over to the customer it will not imply an acquisition of the information per se unless it is more or less readily available for the customer to see. Since it is most likely not more or less readily available the information within the device should not be seen as acquired by the customer.

If the customer would somehow manage to access the information within the external device or web page it would be considered an acquisition of said information. The acquisition would in turn be considered unwarranted as SKF would not have consented to it and it should be obvious for the customer as well, why the acquisition cannot be made in good faith. From evidence perspective the external device is beneficial, since the customer should not have had access to the information within at all.

When installing the bearings using the manual and the external device or similar, the manual part will be considered to be exploited in a legal sense. The part inside the external device is not as obvious. For external part the customer uses the information indirectly by typing a value and receiving an answer. It has been established that indirect use still constitutes exploitation, however, it did not aim at this situation, why the applicability can be questioned. Most likely it will be considered exploitation, in order for the protection to be effective. This implies that when the license is terminated and if the customer has for instance learned the manual and continues to use the device, it will constitute exploitation. Exploiting the manual during the license is warranted as SKF has consented to it. Once the license has expired exploitation is unwarranted, as the consent from SKF has then lapsed.

10.3.4.2 Keeping the Manual

The term acquire indicates that you get access to something that you previously did not have access to. So the question is if the trader secretly keeps the manual, in a licensing situation, when it should instead have been returned to SKF, is this considered an unwarranted acquisition according to the FHL? Fahlbeck states that you cannot acquire something that you already possess, implying that even if you refuse to return the manual, it will not be considered an acquisition according to the FHL since the manual was in your possession to start with. This is the case regardless of distribution model, either digital or analogue, apart from the case of a data-room where manual is only in possession of the trader as long as it is viewed. If the customer somehow manages to access the manual via the data room after the license agreement has expired when the customer no longer should have access, it is an acquisition as something new has been added to the infringer's sphere and it is unwarranted, as SKF would not have consented to it.

Another case is if the customer makes a copy of the manual and keeps it, while returning the original to SKF. Then something new has been added to the infringer's sphere, the copy, why this reasonably must be considered as an acquisition according to FHL. As the manual should have been returned, and no copies be made, the customer cannot have had SKF's consent, either explicitly or implicitly, why the acquisition must be seen as an unwarranted one according to FHL. FHL does therefore provide any protection against the party keeping the manual when it should have been returned, but only when utilising a data room solution or if a copy of the manual has been made.

In the case when keeping the manual is not considered an unwarranted acquisition it might be possible for customer to either transfer the manual to a third party of use it in some way. If the manual is transferred the same will apply as is accounted for below in relation to transferring the manual to third parties. If the manual is used within the company it will however be considered as exploitation according to the FHL as long as it is a commercial utilisation, but there is no requirement for profit. It has above been stated that there is no need that the trade secret is used externally for an exploitation to be at hand, it is enough that it is used internally. Is such exploitation unwarranted? This is negatively defined by the FHL, see section 11.2.4, stating for instance that if SKF would have given consent to the exploitation then this would not be an issue. If nothing is agreed between the parties then the question comes down to if SKF implicitly could have consented to the exploitation. As a licensing agreement, as such, is for a limited time, if the customer continues to use the manual after the termination of the agreement, it will probably be seen as unwarranted if it can be proven that the customer should have understood this, which the customer most likely should have understood. However, stating in an agreement that the manual should be returned or destroyed and no copies are to be made or used after the termination of the agreement would avoid this risk. Marking the manual as 'Trade secret of SKF' would most likely also put the customer in bad faith.

Would keeping the manual be seen as an unlawful acquisition according to the Directive? Given the definition of what should be a trade secret according to the Directive, it most likely implies that when trade secrets are legally transferred from one trader to another, as with the manual, the trade secret will be possessed by both of them. That would in turn imply that, as under Swedish law, you cannot reasonably acquire something that you already possess, why keeping the manual most likely is not to be seen as an unlawful acquisition according to the Directive, regardless of if the manual is digital or analogue. One exception would be if a data room solution is utilised and the customer would manage to access the manual after the license agreement has been terminated,

since every time you access the manual it is seen as an acquisition. Another exception would be if the customer makes a copy of the manual and keeps it, while returning the original to SKF. Then the customer has something new and it therefore most likely seen as an acquisition. Both accessing the data room without authorisation and making copies are actions that explicitly are considered as unlawful by the Directive, why it will be considered as unlawful acquisitions in both cases.

In the case when keeping the manual is not considered an unlawful acquisition it might be possible for customer to either transfer the manual to a third party of use it in some way. If the manual is transferred the same will apply as is accounted for below in relation to transferring the manual to third parties. If the manual is used within the company this will most likely be considered a use according to the Directive. The explicit examples in the Directive of what should be considered as use of trade secrets are very product focused, and relates to production, import, export, etc. which might imply that know-how of the sort that the manual contains cannot be used in a legal sense. However, it is explicitly stated in the proposal for the Directive that different sorts of know-how should be covered by the definition. If this is the case, the only reasonable conclusion must be that it is also possible to legally 'use' such know-how in order for know-how to be protected by the Directive.

Is such use unlawful? It is, in this case, unclear whether any of the three conditions for unlawful use under article 3 is met. The first one is not, since it is not unlawfully acquired. Since there are no contractual provisions there are no confidentiality clause either that could have been violated, however, if the manual is marked with 'Confidential' or 'Trade secret of SKF' or similar it might be enough for the use to be considered unlawful under the second condition. To keep using the manual after the termination of the license agreement is most likely considered a breach of a contractual obligation to limit the use of the trade secret, the third condition, if the customer did it intentionally or with gross negligence. It is however questionable if it is considered as gross negligence to continue to use the manual or if it would be considered as 'normal' negligence. Marking the manual as 'Trade secret of SKF' might affect the judgement so that the customer is considered to have done it intentionally. Using the manual after termination of the license agreement might therefore be an unlawful use according to the Directive, however it is difficult to give a clear answer and therefore have a specified agreement to avoid situations like this is advisable.

10.3.4.3 Transfer

For a transfer of a trade secret from the customer to a third party to be considered as an unwarranted action according to the FHL, the question is if it can be seen as a disclosure according

to the FHL. It is stated that it is irrelevant to whom the trade secret is disclosed, or how it is done, as long as it is to a trader and not a customer. There is however a need for the trade secret to unwarrantedly be transferred from the customer to a new trader and become known for this new trader. Another way would be if the information is unwarrantedly transferred to a new trader by an employee that left the customer for the new trader and brings the information, and the employee has such a position that the new trader knows of the information already by knowing that the new employee has the information. Hence, if the manual is transferred to a new trader, by any means, and this trader gets knowledge of the information this will imply a disclosure that will be considered as a disclosure according to FHL.

The next question is if such a disclosure is warranted or not. Since there is no agreement between the two parties the question comes down to if the customer understands that the manual may not be transferred to third parties. As it is possible to give consent either explicitly or implicitly it should also be possible to have both explicit and implicit confidentiality. If the customer understands that the manual may not be transferred to a third party she is therefore in bad faith, and vice versa. It is however many times difficult to, in the judicial arena, prove that the customer was in bad faith in a case like this, why this is a question that should be addressed in an agreement by using, for instance, a confidentiality clause. If SKF during the whole procedure have acted in a way that implies the wish to keep the manual secret and the customer has also done this up to the time of the disclosure, that the customer will most likely be in bad faith, but it is also difficult to prove. However, in some way marking the manual with 'Confidential' or 'Trade secret of SKF' signs would definitely put the customer in bad faith. Since there is no written agreement between the parties it will be close to impossible to, in the judicial arena, prove the bad faith, in this case, that is needed to make the disclosure unwarranted. Therefore much point to that the disclosure of the manual in the judicial arena might be considered as warranted, unless it has been marked or there are explicit confidentiality provisions in an agreement.

When the manual is transferred to a third party, it is not clear what should be considered a disclosure in the eyes of the Directive. It is established that for it to be any protection, there should not be any requirements as to the amount of third parties the manual was transferred to. That the manual is transferred to a single third party should therefore be enough. It is unclear if the Directive has the same requirement as the FHL has regarding that the transfer must be to a trader or if it would be enough that it is disclosed to a private person. It is also unclear if the third party need to know the information or if it is enough that the third party has access to it. The most reasonable

conclusion is that at least when transferred to a trader, and when that trader knows the information, it will be considered a disclosure according to the Directive.

The question in this case, as with the FHL, is whether or not there is an implicit confidentiality provision between the parties. However, referring to the discussion under the FHL part above, it is to some extent unimportant if such an implicit provision objectively exist or not, since it will be difficult to prove it in the judicial arena. If the manual is marked with 'Confidential' or 'Trade secret of SKF' of if a confidentiality agreement has been entered into the customer will however be in bad faith. Therefore, even if the disclosure in fact is unwarranted, it will in the judicial arena most likely be seen as warranted when there are no written provisions or markings implying the contrary.

10.3.4.4 Learning the Information

If the employees of the customer learn the information within the manual, the question is what happens with the manual from a legal perspective. The manual that SKF still has, and the customer as well, will still live up to the requirements for being seen as trade secrets, the only difference if the employee learns the information within the manual is that instead of having to read it from a screen it is in her head. The circle of people that has access to the manual will not be directly widened by the employee learning the information within the manual as she had access to the manual beforehand, in the long term the circle of people might be extended though. Will the information inside the head of the employee still be protected by the FHL or will it be considered the property of the employee with which she can do whatever she please? It is explicitly stated in the propositionen preceding the FHL that it is irrelevant if the information is written down or resides in the minds of humans for it to be considered as trade secrets. The trade secret definition in the FHL does not cover tacit information, i.e. personal skills, experience or knowledge where "The principle should be that information that anyone with adequate education may convert into practical results should be seen as information in the trader's business. However, is the information tied to the individual so that it cannot, through an instruction or direction, be transferred to someone else then it should be seen as personal information and hence not be part of the trader's business." (author's translation).[144]

The information that the employee learned was in fact transferred to her from the manual, it was possible to write down the information and tell the employee how the installation of bearings

[144] 1987/88:155, p. 35.

should be performed, hence it cannot be seen as tacit information that is the employee's sole property and exempted from the FHL. Also, the acquisition of this knowledge by learning it cannot reasonably be seen as an unwarranted offense as the manual lawfully was transferred to the customer. The conclusion is therefore that the information, even though an employee learnt it, is still considered as a protected trade secret according to FHL. This implies that the provisions of the FHL still are applicable to the information inside the head of the employee. To learn the information in the manual is therefore not an offense according to the FHL, but as the provisions of FHL are still applicable, an exploitation or disclosure of the information might be considered unwarranted and trigger sanctions depending on the circumstances since the manual is licensed to the customer. That is however the case only for as long as the employee keeps working for the customer and is under a loyalty obligation towards her employer. When the employee quits her job she can normally do whatever she pleases with the information, as she is no longer under any loyalty obligations toward her employer, an issue that to a certain point can be addressed by a confidentiality agreement. [145]

Just like the FHL the meaning of the term information has a wide meaning in the Directive and it is also explicitly stated that personal skills and other tacit information should be excluded from what is comprised by the term information. It has already been established, above in relation to the FHL, that the information within the manual is not tacit, and that the employee learning this information does not make it tacit either. Even though the Directive does not explicitly say one or the other the most reasonable conclusion must be that a trade secret does not need to be documented for it to be protected, that it like in Sweden can reside in the minds of humans and be a trade secret as long as it is not tacit information. The fact that the employee learns the information within the manual must therefore reasonably not affect the status of the trade secret, which is still owned by SKF. Also, the acquisition of the manual cannot be an unlawful acquisition either as the employee lawfully had access to the manual.

As the manual still will be considered as a trade secret it implies that the provisions in the Directive will still be applicable to the information inside the head of the employee. To learn the information in the manual is therefore not an offense according to the Directive, but as the provisions of the Directive are still applicable, a use or disclosure of the information might be considered unlawful and trigger sanctions depending on the circumstances. It is unclear what happens if the employee quits her job, since there are no explicit provisions about that situation in

[145] Fahlbeck (2013), p. 322.

the Directive. To avoid this risk a confidentiality agreement should be utilised stating that the employee cannot disclose the manual even after she quit her job.

10.3.4.5 Bankruptcy

It is considered a general legal principle that the bankruptcy estate has the possibility to enter into the agreements of the bankrupt company, or not if that is what the bankruptcy estate wishes to.[146] Even if SKF would not want the bankruptcy estate to enter into the agreement it can still do so by forced entry.[147] Folkesson mentions three situations when a bankruptcy estate might not enter into the agreement, namely if the bankruptcy estate does not have the qualifications of the debtor, if the agreement is of personal character or if the agreement is based on stronger personal trust between the parties, i.e. commission agreements for instance.[148] The legal consequences are then if the bankruptcy estate enters into the agreement the provisions in the agreement are applicable in the relationship between the bankruptcy estate and SKF as before. If the bankruptcy estate does not enter into the agreement the situation depends on distribution model. If the manual, either digital or analogue, was transferred to the customer then the manual should be returned to SKF. If a web-based data room solution is used the customer only has access to the manual when logged in, implying that SKF can erase the user account and there is no risk of misappropriation. As has been established above keeping the manual when it should be returned is not an unwarranted or unlawful acquisition. Hence, neither of these actions will be considered as unwarranted according to the FHL or unlawful according to the Directive, either the agreement is entered into or it is not. However, if the bankruptcy estate performs an unwarranted or unlawful disclosure, exploitation or use that would be considered as actions that would trigger sanctions according to the FHL or the Directive. However, as the sanctions that are possible are damages and a bankruptcy estate generally is insolvent, the possibility to be granted damages is not worth very much. Neither the FHL nor the Directive does therefore provide any protection in case of bankruptcy of the customer, except in the case of disclosure and exploitation.

10.3.5 Conclusion

As is established above in relation to the different risks the protection granted by the FHL or by the Directive is many times not especially extensive and leaves a company unprotected in many situations. The protection is basically limited to the preventive effect that the risk for damages has

[146] Folkesson (2007), p. 129.
[147] ibid.
[148] ibid.

and the criminal actions that might have preventive effect for a person. In relation to each individual case above it is however many times possible to widen the scope of protection of both the FHL and the Directive when complementing them with confidentiality provisions in an agreement or marking the manual with 'Confidential' or 'Trade secret of SKF' to ensure that the customer is in bad faith and not eludes responsibility that way.

It is established that it is possible to claim the manual as property according to both the FHL and the Directive. It can however be argued whether the property claim granted by the FHL and the Directive will be strong in the sense that it grants the proprietor a good control position. The issue with trade secrets is that you cannot be sure that you fulfil the requirements for claiming knowledge as a trade secret until a court has tested it. The reason for this is the lack of an administrative arena. Another issue with trade secrets is the lack of exclusivity over the knowledge they comprise, which lowers the control over the knowledge. The most likely conclusion is therefore that a property claim based on FHL will not be a very strong one.

The question then is whether the property claim in conjunction with the protection offered, will be sufficient to capitalise on the trade secret, i.e. the manual, in a commercial transaction. On a theoretical level it might be a sufficient level of protection, however, practically it does not suffice since the scope of protection for trade secrets is basically limited to prevention by the risk of having to pay damages in the judicial arena. Damages that many times are, if not impossible, then at least very difficult to establish the size of. There is also a big issue with damages and trade secrets, because no matter how much damage you are awarded, if the trade secret is no longer secret there is no possibility of getting it back. The protection for trade secrets in the judicial arena, given by the FHL or the Directive is in other words insufficient when capitalising on trade secrets by transferring them as the FHL and the Directive are designed for static use, i.e. keeping the trade secrets hidden inside the company. Dynamically transacting trade secret requires a high level of control, especially as trade secrets provide no exclusivity over the knowledge, why it has been identified that the control and protection granted by the FHL and the Directive is not sufficient. It is still possible to capitalise on the trade secret, but in order to maintain the value of the trade secret and to create a foundation for a platform for transacting trade secrets by maintaining value and control, neither FHL nor the Directive is sufficient.

For a company of SKF's size there is however the possibility to leverage their size and strength in the business arena to ensure better protection for the trade secret. This implies that a strong player in the business arena can claim that they have better protection than they actually do,

or that more of the information is protected as trade secrets than is actually the case. One reason for this it is that many customers are reluctant to upset a big company like SKF where the position in the business arena works as prevention, i.e. the customer will not reveal the trade secret out of fear, on the other hand many companies are far bigger than SKF where the prevention will not work. Another side of it is that once the trade secret has been revealed a big company will have better chances of getting fair damages from the infringing party due to resources to drive a court case, due to the strong position in the business arena.

11 Block 2 - Contractual Provisions

In the following section different contractual aspects will be reviewed, and later analysed in relation to both cases to improve the protection and control position. Furthermore some aspects on where the line should be drawn for what can be agreed upon between the parties will be investigated.

11.1 Freedom of Contract

A central principle in Swedish Contracts Act (1915:218) is the freedom of contract. The principle states that everyone has the freedom to enter into an agreement, the freedom to not enter into an agreement, and the freedom to agree upon the content in the agreement.[149] There are however limitations to this principle, for example when the law deems it to be necessary to protect a weaker party such as a consumer or employee.[150] Other limitations to this principle are laws that are mandatory and they are not possible to avoid by an agreement. In addition, the principle of freedom of contract does generally not extend to third parties, i.e. it is generally not possible for two parties to contractually bind a third party without her consent.[151]

The scope of the principle stretches to article 36 in the Contracts Act, which expresses the principle of equivalence. The principle states that the whole agreement or conditions can be adjusted or disregarded if they are deemed to be unreasonable when the agreement is signed, if the conditions are changed after signing the agreement, or other circumstances.[152] However article 36 does not state how to analyse whether the agreement or the clause is unreasonable or not, and according to Ramberg and Ramberg's interpretation of the propositionen, an overall assessment of the situation should be made.[153] One of the circumstances is the position of the parties. There are many cases

[149] Ramberg, Christina, Ramberg, Jan, Allmän Avtalsrätt, 9th Edition, Norstedts Juridik 2014, p. 27.
[150] ibid., p. 121.
[151] ibid., p. 19.
[152] ibid., p. 34.
[153] ibid., p. 171.

according to Ramberg and Ramberg where the Supreme Court has annulled or reconciled the agreements between traders and consumers, since the consumer is the weaker party and thereby needs protection.[154] Article 36 is however much harder to apply when both parties are traders, as is identified in NJA 1979 s. 483. The case considered an expected exclusion clause in a standard agreement that was very extensive and where the distributor was a listed company while the smaller enterprise was a family owned company. The supreme court stated according to Ramberg and Ramberg, that "the circumstance that one of the traders is a small enterprise compared to the other party, does not constitute, in itself, evidence for that party to have an inferior position" (authors' translation).[155] The Supreme Court did not reconcile the agreement. The reasoning seems to be that the judicial system should pose minimum obstruction to trade and that this is something best managed by the parties themselves.

11.2 NDA

NDAs are not regulated by any special law and therefore it is the Contracts Acts, where freedom of contracts is the starting point. There is no form prescribed by law and NDAs can therefore be entered both orally and written. A written agreement is however preferable from an evidence aspect.[156] Tonell compares the NDA as a protection measure with FHL and concludes that the NDA is only applicable between the parties that have entered into it while it according to FHL article 8 is possible to act against a third party.[157] Tonell thereafter states that this is more important within larger corporate organisations "[w]here it is not possible for all concerned parties to know of all the secrecy commitments within the organisation" (authors' translation).[158] It is therefore important that the scope of the secrecy is set out in the NDA.

It is possible for a trader to enter into NDAs with her employees. This is often done through the employee contract but this secrecy commitment can also be entered in a separate agreement.

Since there is no special law regulating NDAs, there is no special law regulating whether or not they can be adjusted or identified as void. This is done by article 36 of the Contracts Act, as mentioned above. Any NDA, or content of such agreement, e.g. the length of the secrecy commitment, that is found unreasonable can be nullified or adjusted. Tonell states that in the situation where the parties are traders the scope for something to be unreasonable is slim, implying

[154] ibid., p.121.
[155] ibid.
[156] Tonell (2012), p. 58.
[157] ibid., p. 59.
[158] ibid.

that more or less any NDAs can be entered into.[159] However, in situations where the trader has drafted long secrecy commitments, or even infinite secrecy commitments, the trader should state the reasons for this in order to not get them adjusted or nullified.[160] When the trader enters into secrecy commitments with her employees the situation is different. The employee is often considered as the weaker party and therefore in need of extra protection. However, Tonell concludes that the employer's interest to protect her trade secret should be taken into consideration. This means that in the situation where the employee leaves the company a more favourable assessment from the employer's perspective can be done according to Tonell.[161]

Tonell gives two examples for how a NDA can enhance the protection given by FHL, one where the trader has entered into a negotiation with another trader and the other one when an employee leaves the company.[162] Article 6 of FHL gives that a trader is liable for exploiting or revealing a trade secret, which she has been given in confidence during negotiations. If the trader has signed an NDA the party who has given the information can fairly easily show that there has been a breach, i.e. the trader was in bad faith, and that article 6 is applicable. Without an agreement this would be hard since the burden of proof is, according to FHL, on the plaintiff.[163] In the situation where an employee leaves the company, her loyalty obligation towards her former employer ends. Therefore the risk is that the employee reveals secret information after her employment. Article 7 of FHL is set to deal with these risks. However, according to section 2 of article 7, extraordinary reasons are needed in order for the former employee to be liable. Fahlbeck and Tonell state that a breach of a specific NDA is such an extraordinary reason.[164]

11.3 Implications of FHL on Secrecy Provisions

The question whether or not the FHL limits the possibility to agree on secrecy has been encountered throughout the literature. The question affects the contractual protection that can be offered. Tonell is of the opinion that "[i]t is clear that the parties cannot extend the scope of FHL by using wider definitions of which information should be covered by the NDA than the legal definition as set out in article 1 FHL" (authors' translation).[165] Tonell states that the same is

[159] ibid., p. 62.
[160] ibid.
[161] Tonell (2012), p. 63.
[162] ibid., p. 64.
[163] ibid.
[164] ibid., p. 65; Fahlbeck (2013), p. 465.
[165] Tonell (2012), p. 61.

applicable in relation to article 2 of FHL since both article 1 and 2 are mandatory. Therefore any secrecy commitments that extend these articles can be void. Fahlbeck is of the same opinion and states that "[a]greements that state secrecy in situations that are not considered as unwarranted according to article 2 are void"[166] (authors' translation). Considering article 1, Fahlbeck has the same reasoning as Tonell that article 1 is mandatory and the definition can therefore not be extended.[167] However, as Tonell states, it is a different question whether or not the parties can, on contractual grounds, regulate and limit the use of a party's information, even if that information would not be considered as a trade secret according to FHL.[168] Tonell is of the opinion that as long as the contractual agreement is not unreasonable the traders are free to contractually regulate the use of party's information. Fahlbeck on the other hand states that such agreements are void.[169] Wainikka's conclusion is however not as direct, since she states that the legal position is uncertain.[170] Hence, it might be possible to regulate and limit the use of a party's information even if it is not considered a trade secret according to article 1 FHL.

11.4 Penalties

Adlercreutz and Gorton states that penalties are in advance standardised damages, with the double-edged function of both facilitating determination of an appropriate level of compensation as well as leverage against the other party of the agreement to ensure she fulfils her contractual obligations.[171] The parties generally decide that in a specific action or case a sum of money should be paid to the other party, e.g. if a licensee discloses a trade secret the level of compensation can be determined beforehand avoiding difficult and time consuming assessments of the size of the damage that is required for damages to be awarded.[172] However, penalties may also work as a limitation of the responsibility, in cases when the penalties are set to a low level, which was the case in NJA 2010 s.629.[173] In such a case the penalty may be seen as a substitute for fulfilling the contractual obligations.[174]

---

166 Fahlbeck (2013), p. 75.
167 ibid.
168 Tonell (2012), P. 61.
169 Fahlbeck (2013), p. 75.
170 Wainikka, (2010), p. 62.
171 Adlercreutz, Axel, Gorton, Lars, Avtalsrätt 1, 13th Edition, Juristförlaget i Lund, 2011, p. 316.
172 ibid.
173 ibid., pp. 316-317.
174 Gorton, Lars, Samuelsson, Per, Kontraktuella Viten, Studier i rättsekonomi - Festskrift till Ingemar Ståhl, 1st Edition, Studentlitteratur, 2005, p. 76.

Penalty clauses are under Swedish law generally binding unless they are found to have unreasonable effects, in which case they can be adjusted according to article 36 Contracts Act.[175] A penalty that is unreasonably high might be lowered or overridden entirely, the penalty might also be increased if the size of the penalty is seen as an unreasonable limitation of the compensation, however, Adlercreutz and Gorton argues that it in practice is rare that the penalty is increased.[176] Penalties can be used for positive contractual obligations, such as late delivery, error in the product etc., where the penalty will work as a substitute for damages, but it can also be for negative contractual obligations as contractually determined compensation for breach of for instance secrecy or competition clauses.[177]

12 Analyse of Block 2 - Embedded Knowledge

As mentioned, the most imminent threats are dismantling the sensor, acquiring information without dismantling it, transferring it, stealing it, and bankruptcy situations. The following will analyse how these threats can be reduced using the agreement as a legal tool, which is the second block of the foundation for the platform.

12.1 Dismantling the Sensor

Dismantling the sensor, in order to acquire the secrets kept within, is – as mentioned – the most imminent risk. The contract can be used as an effective tool in order to prohibit the buyer or licensee to commit this act by stating that any attempts to dismantle the sensor is a breach of contract with penalties as sanction. Since the freedom of contract is the starting point this is most likely not identified as unreasonable especially since SKF has a great interest in keeping the sensor secret. Even if it is fairly easy to agree upon such a clause it is harder to ensure that the buyer follows the agreement. This is a general deficiency with agreements that is hard to overcome until it is too late, i.e. the buyer has already breached the contract and accessed the knowledge. Therefore the penalties should be set very high in order to have a preventive effect.

Situations where the buyer thinks she can legally dismantle the sensor can arise. One can imagine the situation where the sensor stops functioning and the buyer tries to open the sensor in order to identify what is wrong. These situations should be designed as a breach of the contract in order to reduce the risk for the buyer to acquire the information within. Penalties as a sanction

[175] Adlercreutz, Gorton (2011) p. 317.
[176] ibid.
[177] Gorton, Samuelsson (2005) p. 89.

should be connected to this breach. The design of the clause should be as such that SKF's own technicians shall do any repairs necessary in order for the sensor to function properly. This clause is identified as not only good from a control position but also from a business perspective, since it offers more value propositions for the buyer in form of a service.

In order to enhance the protection given by this clause it should be connected to a warranty as well. It is very common to state that if any attempts to dismantle a product are committed, the warranty given by the trader ceases to exist. This is identified as a clause that has the potential to refrain the buyer to dismantle the sensor if the warranty is favourable, and should therefore be included in the contract.

An agreement that the trader cannot dismantle the sensor might not be enough. The situation can arise where the employees of the buyer tries to dismantle the sensor without knowing it is a trade secret. The employee would then be in good faith and not liable for any breach. Therefore a clause stating that the customer guarantees that her employees are under secrecy provisions should added to the agreement. By doing this there can be no doubt that the employees that have any connection to the machine are in bad faith when attempting to dismantle the sensor.

The above stated contractual obligations affect the protection given by the FHL and the Directive. The obligations help ensuring that the circle of people is kept as limited and controlled as possible. The obligations also show that SKF fulfils the objective and subjective criteria set out in the FHL prerequisites by addressing to the customer that the knowledge should be kept secret.

12.2 NDT

Acquiring the information without dismantling the sensor can be described as the first step in order to dismantle the sensor. However, in order to avoid misunderstandings it should be stated in the agreement that using any methods to acquire the information within the sensor, without dismantling it per se, should be considered as a breach of contract with penalties as a sanction. This clause suffers from the same problem as the one identified above, it is hard, probably even harder to identify that there has been a breach of contract before it is too late. It is hard to establish that somebody has used for example X-ray or sound waves in order to understand how the sensor is constructed.

This contractual obligation affect the protection given in the first block by addressing towards the customer that the knowledge within the sensor is a trade secret of SKF, thereby fulfilling the objective and subjective criteria of the prerequisites in the FHL. The obligation also helps keeping the circle of people limited and controlled.

12.3 Transfer

In order to reduce the risk of the buyer transferring the sensor to a third party the buyer should sign an NDA as soon as the negotiations are initiated. By doing this, the trader will be in bad faith, and can therefore not claim that she did not know that it was a secret. The act of transferring the sensor to a third party should also be identified as a breach of contract sanctioned by penalties. However, as with the other clauses, the problem is to know whether or not this clause has been breached.

This contractual obligation is important because it is very intertwined with the first block. The analysis under block 1 shows that trade secrets can be acquired in good faith. When so it means that the customer is not reliable for any infringements done. By utilising this contractual obligation it is ensured that the customer is in bad faith when she acquires the sensor and thereby reliable for any infringements. This contractual obligation shows how important it is to address different protective measures in order to utilise the protection given by the FHL and the Directive.

12.4 Stealing

In order to make sure that the sensor is not stolen provisions on how it should be safeguarded should be agreed upon. It is hard to analyse this clause in detail since it depends on the circumstances in each case. However, a general clause stating that the buyer should take reasonable actions to safeguard the sensor should be added in the contract.

Even though this obligation does not affect the first block directly it has an indirect affect by trying to keep the circle of people as limited and controlled as possible in the long run. The obligation also puts pressure on the customer to maintain the secret character

12.5 Bankruptcy

The risk of a trader entering into bankruptcy is not as easy to address with contractual agreements. In order to avoid this situation traders usually agree upon a "change of control" clause. This means that, in a situation where the trader enters into bankruptcy and the official trustee takes over operations, the contract is nullified. However, Folkesson states that the trustee can enter into almost any agreement deeming such a clause inoperative.[178] Therefore another approach is required to address this question. The best approach is a proactive approach where commitments to keep SKF informed about the economic status of the acquiring trader. However, this is probably not easily agreed upon since a company is most likely not prone to hand out information about their economic situation. In a licensing situation it is probably easier to state that if the royalty is not paid on time,

[178] Folkesson (2007), p. 129.

the sensor should be returned to SKF. Much points to that when the buyer is ceasing to fulfil her commitments, the risk of her entering into bankruptcy is higher. With this clause the sensor will not get into the hands of the official trustee and in the long run in a third party's hands. However, there are deficiencies with such a clause as well. One can imagine the scenario where the buyer prioritises the royalty payments for the sensor while actually her economic situation deteriorates fast without SKF knowing.

Using contractual provisions in order to prevent the bankruptcy scenario affect not the claim made in block 1. It neither strengthens nor decreases the protection given by the FHL or the Directive. However, it does facilitate the transaction of the sensor since this situation is identified as an imminent risk.

12.6 Conclusion

Since the starting point is freedom of contract the above mentioned content of an agreement are most likely identified as reasonable when the parties are both traders. It is another question whether or not a buyer would accept these clauses, i.e. from a business perspective it might be hard to implement some of the clauses. Moreover, an agreement is identified as crucial in order to protect the trade secret but there are also problems with it. With the agreement SKF have to rely on its preventive effect since even if the buyer or licensee breaches the contract it is hard to know when she breaches it. Often this will come to SKF attention too late, i.e. when the breach has already been committed and the buyer or licensee has acquired the secret information. As soon as the buyer or licensee learns the information the exclusiveness is destroyed since it is impossible to erase – take back – what someone has learned.

As mentioned, it is hard to establish the damage from an infringement. Using a contractual agreement with penalty as a sanction is an easier approach since both parties know in advance the economic consequences of a breach. A breach of a clause connected with a penalty means that as soon it is established that there has been a breach, the breaching party has to pay the set penalty. One question that is interesting and affects the protection is how high the penalties should be set. Because there is freedom of contract this can be set as high as the parties can agree upon. It is identified that SKF has a great interest to keep the sensor secret, which justifies higher penalties. However, high penalties might be contra-productive to business since high penalties can scare traders, especially SMEs, to enter into the agreement. High penalties are also more likely to be adjusted or nullified if they are identified as unreasonable according to article 36 of the Contracts

Act. Given that SKF has a legitimate interest in keeping the information secret, the starting point should be to set the penalties high.

The analysis shows that the contract only has a preventive effect. The conclusion is therefore that there needs to be incentives for the buyer to follow the contract. The penalty is one method to incentive the buyer to not breach the contract. Another solution that could be utilised is to draft the contract so that the majority of the royalty is paid in the beginning of the agreement. The heavy investment the trader needs to commit herself to in the beginning of the agreement creates an incentive not to breach the contract, since it would be too expensive to breach both the agreement, i.e. paying high penalties, and to pay the high royalty. A depreciating royalty scale is often used in license agreement and should pose as a minor challenge to agree upon.

Petrusson states that it is possible to claim properties by simply using contracts since the assumption is that the contract will be upheld in the judicial arena.[179] Therefore the proposed licensee agreement above is yet another property claim, which is separated from the FHL and Directive claim made in 'Block 1'. However, even if there are well developed institutions that safeguard that the contract is fulfilled, the problem is – as mentioned in the paragraph above – that the contract is only a preventive measure that can be breached in order to gain the knowledge. It is the author's belief that in order to create a foundation for a platform for transacting physically manifested knowledge through trade secret protection, the agreement and the protection given by FHL or the Directive is not enough to ensure dynamic use of the trade secret.

Following Petrusson's and Heiden's theory, the right given by the contract can be used and accepted by the market actors and society. However, it needs to be mentioned that as much as FHL is applicable in Sweden, the NDA can be interpreted differently in other countries than Sweden, i.e. Sweden is only one of several business arenas. Therefore the contract might need to be changed depending on which country, i.e. which business market the sensor is sold in.

The analysis finally shows that the contractual provisions are intertwined with the protection given in the first block, and many times necessary in order to enable the protection. Unsurprisingly the conclusion is therefore that in order to transact trade secrets there needs to be contractual provisions protecting them.

[179] Petrusson (2004), p. 115.

13 Analysis of Block 2 - Openly Available Knowledge

As have been stated above the most imminent risks identified in relation to transferring a manual to a customer is that there is too much information within the manual, that the customer keep the manual when it should have been returned, that the customer may in turn transfer the manual, that the customer may learn the information within the manual and that the customer can enter into bankruptcy. In the following will be analysed how the legal tools presented above in relation to block 2 can be utilised to lessen said risks and how they can affect the protection granted by FHL and the Directive.

13.1 General Provisions

It has been established above that freedom of contract is the general principle unless anything else is explicitly stated elsewhere. In the following will therefore be analysed what different contractual means are available to facilitate the transfer of trade secrets in the form of a manual to a customer. It should however be emphasised that it is not possible to contractually bind a third party against her will. Therefore risks in relation to such situations, such as that employees might not be bound by the provisions in the agreement straight away, must be secured by other means such as that the customer guarantees that the employees follow the provisions in the agreement too. Such a provision would not affect the protection according to FHL and the Directive. The provisions in the agreement between SKF and the customer regarding other issues might however affect these legal acts, which will be reviewed in connection with the analysis below. Initially general provisions that are applicable for all risk will be addressed followed by risk-specific provisions.

13.1.1 NDAs

Non-disclosure agreements or similar secrecy or confidentiality provisions have the advantage of making explicit how a party may and may not handle the information she has received, for instance making copies should not be allowed. Also NDAs as such are reasonable in the eyes of article 36 Contracts act, however, if too lengthy it might be considered as unreasonable. NDAs do also have the benefit of fulfilling the activity criterion under FHL and most likely the Directive. It does also put the party in bad faith, implying that it is easier to prove a disclosure is unwarranted according to the FHL or unlawful according to the Directive, where for the Directive one specific provision for responsibility is if the party has violated a confidentiality provision. For the NDA to provide a full cover it should be signed already during negotiations, and also cover arbitration and arbitration awards so as to ensure that at no point during the collaboration the trade secrets are revealed. If no

secrecy is agreed upon during arbitration the parties are free to disclose all the information, as was decided in the case NJA 2000 s. 538. In relation to this it should therefore be noted that when transferring trade secrets the parties should always agree to settle any disputes by arbitration to allow the proceedings to be secret. However, regardless of situation, if there is no NDA, or if it is expired, the information might still be considered as a trade secret and be protected by either FHL or the Directive.

Being in SKF's position one should always strive for as long confidentiality provisions as possible to ensure the trade secrets are not lost. If being between equal parties it is under Swedish law also unlikely that it would be considered unreasonable only because of the duration in time. However, from a business perspective a party might not be keen on signing a far-reaching confidentiality clause. There is also the issue that it might be difficult to know when a party has violated an NDA, which is the same issue as with relying on trade secret legislation like FHL or the Directive, the customer might have spread the manual to all of SKF's competitors without SKF knowing of it. Therefore, even if an NDA provides several benefits, one should still choose customer with care, a customer that can be trusted.

13.1.2 Penalties

As has been established it is very difficult to determine the size of the damage that has been caused if a trade secret has, for instance, been unwarrantedly disclosed according to FHL. This is a big weakness of the protection granted by FHL and the Directive. The most convenient way to avoid this weakness and the difficult, and many times time consuming, enterprise of determining the level of damage is to have pre-set penalties in the agreement. However, it does not affect either the claim or protection granted by FHL or the Directive.

For the most severe offenses the penalty should be set really high, and for less severe offenses the penalty should be set lower. Big penalties should legally not be an issue as long as the parties are both traders and 'equally powerful', they are supposed to know what they are getting into and therefore it is not seen as unreasonable. It should nonetheless be noted that from a business perspective it might be impossible to have such big penalties if the customer will not accept it, especially for SMEs which might be frightened by the high penalties. Setting too low level of penalties is however also a risk since it may be seen as a limitation of responsibility, but it has the upside of from a business perspective as it would be easier to tolerate as a customer. The penalties should therefore be set as 'high as possible' since the risk of having the penalties seen as

unreasonable and set down is most likely less than the risk that the penalty is set too low and seen as a limitation of responsibility.

13.1.3 Access to Information

The risks that the manual might be transferred, kept or learnt, are all relating to individuals. If there are no persons accessing the manual these risks will be more or less avoided. However it is also possible to limit the risk by minimising the circle of people that has access to the information in the manual. This can be done contractually by explicitly stating who should have access to the manual, either digital or analogue. This will also have the benefit of effectively limiting the circle of people that has access to the information while fulfilling the activity criterion according to FHL and most likely the Directive, ensuring that it will still be considered as a trade secret. If the manual is transferred outside this circle it is a disclosure that is unwarranted according to both FHL and the Directive. This provision therefore increases the effectiveness of the protection from said legislation. If this provision is violated it is however very difficult for SKF to become aware of the violation.

13.1.4 Payment

One way to incentivise a customer to not leak the manual or otherwise violate the agreement is to use a payment method for a license deal that will make the customer reluctant to take any risks. The method that should be used is to divide the payment into two different parts, one part that is an up-front payment, and one part that is royalty based and is due every month or quarter or similar. From a business perspective it should not be difficult to convince a customer of a model like this, at least if the agreement is for a specific amount of years since that would imply that a model with only royalties would end up with the same cost in the end. The up-front payment should be set at a level that makes it, together with penalties, more expensive for a customer to disclose the trade secret than staying as licensee, regardless of when the disclosure occurs.

This model affects neither the claim nor the protection granted by FHL or the Directive. It does only provide incentives for not violating the provisions of the contract.

13.2 Too Much Information

The risk posed by having too much information within the manual is a risk that cannot be remedied by neither legal nor contractual measures. The only solution for this risk is to, in some way, limit the amount of information given in the manual.

13.3 Keeping the Manual

It has been identified that one of the risks in a licensing situation is that the customer keeps the manual when it should be returned. To begin with there is a need for a provision in the agreement stating that SKF will retain title to the trade secret, i.e. the manual. It should also be agreed that the customer should return the manual upon termination of the agreement. This provision should be used in conjunction with penalties, is the manual not returned, or if a copy is kept or similar, then the customer is liable to pay a penalty. The level of penalties should be on the upper part of the scale since it would imply that SKF would lose the control over the manual. There ought also to be a provision in the agreement stating what the customer may and may not do with the trade secret under the agreement, to set the outer boundaries.

The provisions in the agreement stating what the customer may and may not do with the manual can serve as an effective way proving that an unwarranted offense according to FHL or unlawful offense according to the Directive have occurred. This is the case when for instance the provision states that after termination of the agreement the customer is not allowed to continue to use the manual. If the customer does this anyway, it can easily be proved that it is a violation of FHL or the Directive, if SKF ever finds out about the violation that is. Stating how the manual may be used in the agreement will also fulfil the activity criterion according to FHL and most likely the Directive.

As has been established above, even if the manual includes some information that is publicly available and therefore is not considered as trade secrets, the manual as a whole must reasonably still be seen as a trade secret. For information within the manual that is not trade secrets it is unclear whether it is possible to limit the management of said information from a legal perspective. Due to this uncertainty there is a possibility to claim that it is possible to limit the management of such information and bet on that your claim is the right one if a court tries the question. Either way it is likely that if the question will be tried by a court it will not be in the immediate future, during which time it is possible to leverage the uncertainty in this question. However, the manual as such may without doubt be agreed upon since it as a whole will be seen as a trade secret.

13.4 Transfer

To address the risk that the manual might get transferred to a third party it should be a provision in the agreement stating that the customer may not transfer the manual to anyone that is not part of the agreement, i.e. to any third party. To ensure the effectiveness of this provision it should be used in conjunction with penalties, which should be set on the top level of the scale of penalties as

transferring the manual to a third party is the most severe violation of the agreement, at least from a trade secret perspective since the circle of people might become too big for it to be considered secret.

To begin with this provision will fulfil the activity criterion according to FHL and most likely the Directive, since it aims at maintaining the secret character of the manual. If the manual is transferred and thereby violating the contractual provision it is obvious that it constitutes an unwarranted disclosure according to FHL and the Directive. Such a provision will therefore increase the effectiveness of said legislation. It may nonetheless be difficult to become aware of that the disclosure has ever occurred.

The manual might get stolen, for a digital manual either by hacking an electronic device or stealing the entire device on which the manual is stored or for an analogue manual by simply grabbing and walking away with it. Therefore there should be a provision in the agreement between SKF and the customer that the customer should take all reasonable protective measures or similar to ensure it is not stolen. Having a general provision as the one mentioned would make it difficult to sanction, however, if stated in the contract that specific protective measures should be taken, then they should be sanctioned by penalties to ensure observance. Such provisions will not affect the protection or claim according to FHL and the Directive.

13.5 Learning the Information

One could imagine a provision in the agreement between SKF and the customer stating that the customer's technicians are not allowed to learn the information within the manual. However, such a provision would not avoid the risk that the technicians learn the information within the manual, and it would be very difficult to prove that it had happened for any sanctions to be applicable. On top of this it is highly likely that it would be considered unreasonable according to article 36 Contracts acts as many times you cannot decide what to learn and not, if you install bearings using the process described in the manual over and over it is impossible not to remember anything of the procedure after a while.

A better solution would be to, in the agreement between SKF and the customer, state that the employees of the customer that will use the manual should be under secrecy obligations that extend also after the employee has left her job. Such an obligation will fulfil the activity criterion of FHL and most likely the Directive. If the obligation ends when the employee leaves her job it will be a big risk, since the employee may do whatever she please with the trade secret without sanctions according to article 7 FHL, unless in very severe cases. Violating a specific secrecy provision is such

a severe case, as has been noted above. As mentioned above the length of such provisions might be problematic if being too long, which especially has to be taken into consideration when it comes to employees. However, if it is possible to present a good motivation for the length it lowers the risk for problems associated with this. Also it should most likely lower the risks for problems if the secrecy provision is very specific and only covers the manual. This provision should be sanctioned by penalties, in order for the customer to actually ensure that the employees are subject to such secrecy obligations, as the agreement requires. It should be noted that even if a secrecy provision have been violated it is many times difficult for SKF to prove, or even become aware of, the violation, making it difficult to protect oneself against an employee learning the manual.

13.6 Bankruptcy

If the customer of SKF would go bankrupt, the question is if it would be possible to contractually prevent the bankruptcy estate from taking control over the manual. If the manual was sold from SKF to the customer it is the property of the customer and SKF can do little about this. If the manual is licensed instead the question becomes if it would be possible to, on a contractual basis, prevent the bankruptcy estate from entering into the agreement by using for instance a change of control clause. As has been noted above under section 10.3.4.5, a bankruptcy estate may enter into an agreement even if SKF would not like to be part of that agreement. According to Folkesson, the same applies to change of control clauses, if the bankruptcy estate wants to enter into the agreement, the change of control clause cannot prevent it from doing so.[180]

Better is instead to find solutions that will end the relationship before the bankruptcy, or at least preserve SKF's interests. If the royalty payment is due every month, and this is not paid within a certain period of time, SKF should have the possibility to terminate the agreement. If this period is too short it might be seen as unreasonable and if the customer prioritise the payment to SKF over other invoices it might not provide any protection at all. If it is possible to terminate the agreement with a couple of months term of notice it would be possible to terminate the agreement if the customer would show signs of insolvency. This model would require that the agreement may be terminated by SKF without stating any specific reasons and that SKF have access to the customer's continuous financial data to be able to notice signs of insolvency. A solution like that might be difficult to use from a business perspective, since the customer and the survival of the agreement would be subject to SKF's notion and the customer might not want to share the financial

[180] Folkesson (2007), p.129.

information with SKF. The model with a big up-front payment has the positive implication, apart from incentivising a party not to leak the manual, that SKF would be certain to at least have gotten that payment out of the relationship, since bankruptcy for the customer may make it difficult for SKF to get paid.

Neither of the contractual measures trying to address a potential bankruptcy situation will affect either the trade secret claim or the protection granted by FHL and the Directive.

13.7 Conclusion

As a general conclusion it can be said that not only relying on the FHL or the Directive, but also using contractual obligations will facilitate the transfer of trade secrets and ensure a stronger foundation of a platform. It will make it clearer what is actually protected and from what type of actions by utilising provisions on how the manual may be used, and by whom, and confidentiality provisions. This type of provisions will also ensure that the protection granted by FHL and the Directive is actually available and not only a facade. It will facilitate claiming knowledge as trade secrets according to these legal acts, for instance by fulfilling the activity criterion according to FHL and in most cases the Directive. The conclusion is therefore arrived to that in order to be able to transact trade secrets at all there is a need for contractual provisions to protect them.

By complementing the provisions with different levels of penalties the effectiveness of said provisions will be made more secure. Utilising big up-front payments will allow SKF to have a more secure position, as it will deter customers from violating any of the provisions in the agreement. It is also recognised that it might be possible to agree what may and may not be done with information that falls outside the scope of the FHL, however as the doctrine provide contrarious opinions as to whether this is possible or not caution should be exercised in relation to these matters. As the contractual provisions are described from a Swedish perspective there are most likely differences in other legislations that need to be taken into consideration when transferring the manual, unless the contract is explicitly governed by Swedish law which might not be possible in every case from a business perspective.

Petrusson states that one way to claim intellectual properties is to in the business arena utilise contracts since the assumption is that the contract will be upheld in the judicial arena, i.e. a judicial court.[181] This implies that SKF may utilise the legal contract as a property claim of the knowledge within the trade secret. However, both trade secret legislation and contracts are merely

[181] Petrusson (2004), p. 115.

preventive measures that provide incentives, mainly financial, for the party not to violate the provisions in the law or the agreement. If the trade secret is disclosed money cannot change that fact, and many times it is difficult to recoup the investment in the information by damages or penalties from the disclosing party. It should also be emphasised that it many times might be impossible to even become aware of that the customer has violated the contract, implying that even if a high penalty would provide some compensation it would not help if the violation of the contract never becomes known by the proprietor of the trade secret. It is therefore obvious that the protection granted by legal contracts as such is not sufficient in order to capitalise on trade secrets such as the manual when dynamically using the trade secret.

14 Block 3 - Practical Measures for Protecting Embedded Knowledge

This block investigates what practical protection measures can be used for protection the sensor in relation to the imminent risks.

14.1 Dismantling the Sensor

Dismantling the sensor is identified as the most imminent risk. Below are presented several measures on how to lower this risk. Some of the protective measures address not only the risk that the customer dismantles the trader but also some of the other identified imminent risks.

14.1.1 Moulding

As shown in Figure 7 the components and their relation to each other is what need to be protected. One way to protect the information is to mould the inside of the shell, with the components within, see Figure 8, of the sensor and thereafter sealing it. This solution has been used to mould ECUs with plastic materials making it hard to access the information within. "ECU (Engine Control Unit) is a type of electronic control unit that controls a series of actuators on an internal combustion engine to ensure optimal engine performance."[182] If someone tries to open the ECU they

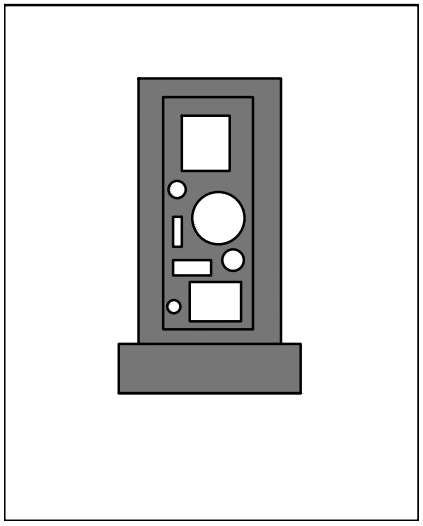


Figure 8 - Moulding the Sensor

[182] Stackoverflow, "How are Engine Control Units (ECU) of high speed racing bikes coded?", retrieved 24/04/2014 from, http://stackoverflow.com/questions/23635784/how-are-engine-control-units-ecu-of-high-speed-racing-bikes-coded.

more or less have to destroy the unit itself in order to get the information. It is identified that by destroying the unit the infringer might get information about which components are used although they most likely are broken by that time. However, by simply destroying the unit it will be hard to understand the relations between the components. It is therefore identified that, depending on how 'precise' the infringer can destroy the moulding, some of the information might still be unknown for the infringer.

There are however potential problems with moulding the sensor. Question is whether or not the components will operate as they are supposed to when they have a cask consisting of plastic material surrounding them? It is however not a question that will be further investigated since it lies outside the scope of this thesis.

Bosch uses this solution in order to protect their trade secrets they have in their ECUs. They mould their ECUs and then sell them to Volvo, without Volvo knowing what is in them. However, this solution is not 'bulletproof'. In the Bosch case, Eriksson AB successfully opened one of the ECUs and discovered that the material within was very cheap and simply arranged in proportion to the price charged by Bosch. A quick Internet search shows that a company called ACtronics, with headquarters in the Netherlands, specializes in dismantling ECUs in order to repair or modify them.[183] It is therefore established that this solution is not bulletproof but only hinders the infringer, i.e. it makes it harder for her to access the trade secret.

Utilising moulding as a protective measure affects both the protection given in block 1 and 2. First of all moulding the sensor enables SKF to keep the secret by limiting the possible circle of people. It is furthermore possible to connect this practical measure to a contractual provision, which states that any attempts to destroy the moulding are a breach of contract. The moulding also acts as a measure showing that SKF fulfils the objective criterion as set out in the FHL. It furthermore obstructs the customer to infringe the sensor by acquiring, disclosing, or exploits it.

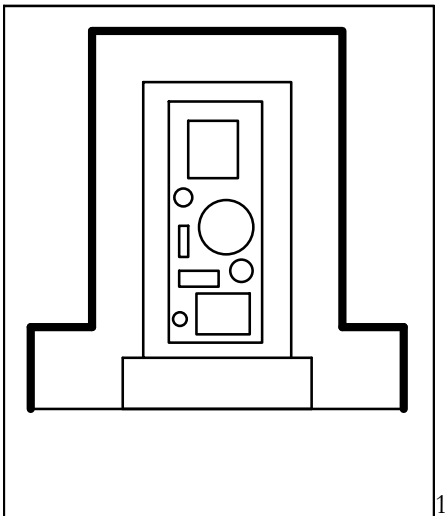
14.1.2 Embedding

As identified in section 7.1, the sensor can either be mounted or embedded within the bearing, if the bearing is big enough. Embedding the sensor is one way to protect it. In order to understand how this protection works, there is a need to describe the environment in which the bearing is utilised. The bearing is an element of a machine that constrains relative motion and reduces friction between moving parts to only the desired motion. It is an important element of a machine and if broken,

[183] Youtube.com, "Ombyggnad av en Bosch ABS-enhet - ACtronics", retrieved 24/04/2014 from: https://www.youtube.com/watch?v=mCanmgjx-M0.

forces the whole machine to stop. If the sensor and the bearing is an element of a an important machine performing industrial operations or reducing friction in a wind power station, a shutdown will have significant economical impacts. This leads to the conclusion that if it is possible to embed the sensor within the bearing, the trader will need to shut down the operations for the time to remove the bearing, remove the sensor and analyse it in order to understand it. The manufacturer then has to return it into the machine in order to start up the production again. These are major decisions that will most likely be very expensive since it is not possible to remove the sensor without shutting down operations. In order for this strategy to provide the best protection possible, SKFs own technicians should install the bearing within the machine. This is also the scenario in some cases but in the majority of cases the trader who purchases the bearing installs it herself. Another deficiency with this strategy is that manufacturers often have scheduled shut downs in order to perform maintenance. During one of these scheduled shut downs there is a window for the manufacturer to analyse the bearing. However, to embed the sensor is still identified as a better solution than only needing to mount it on the machine itself since embedding has a more preventive effect. When mounted, the trader does not need to shut down operations in order to analyse the sensor, i.e. the costs for removing the sensor are low.

In the situation where the sensor is embedded within the bearing SKF should always try to be the one installing it. By doing so this protective measure will ensure that the circle of people is kept at a minimum, thereby enabling the protection offered from block 1. It is identified that in many situations the customer wants to install the bearings themselves. This lowers the strength to some degree but embedding the sensor per se limits the circle of people and increases the control. This practical measure also obstruct the customer from transacting, making it a practical measure that lowers the risk from the sensor being transferred to a third party as well. This measure also obstructs the sensor from being disclosed, exploited and acquired, thereby enabling the protection given by block 1.



14.1.3 Secondary Shell

Another way to protect the sensors from being dismantled is to create a secondary shell covering the sensor and its original plastic shell. By creating a secondary shell that consists of harder material than plastic, e.g. steel, it will be

harder for the infringer to acquire the information within. Today many of the sensors that are used by SKF are mounted on machines by a single mounting stud. With a secondary shell, the shell itself will need to be mounted by several mounting studs in order to make sure that the customer cannot remove it easily. If it is possible to mount the sensor by using special tools only available at SKF it is identified as the best solution when mounting the sensor. It will make it harder for the infringer to open the second shell, see Figure 9.

This solution is identified as very feasible since it is fairly easy to construct and use. With this solution there is no need to interact with the components and thereby possibly hinder them from performing optimally. However, it is not identified which thickness the secondary shell should have. Generally a thicker shell implies that it is harder to access what is inside of it. The problem might be that it is too thick and unintentionally intervenes with the sensor or with the sensor's ability to transmit data. This is not further investigated since it is not covered by the scope of this thesis. As with the moulding solution, this solution is not bulletproof but only makes it harder for the infringer to access the information.

First of all utilising a second shell does not only protect the sensor from being dismantled, it also obstructs the customer from easily transferring it to a third party. A secondary shell also facilitates a more limited and controlled circle of people and thereby enabling protection from block 1. It is furthermore a measure that lowers the risk that the sensor is stolen or exposed to espionage.

14.1.4 Self Destruct

Given that the sensor can either be mounted on the machine containing the bearing or, if the bearing is large enough, contain the sensor within the bearing, a design which destroys the sensor, if opened in a wrong way, can be one preventive measure. In an interview with Pernilla Hallberg, customer administrator at ACtronics, it was confirmed that when an object, that has these protective measures, is the most complicated one to dismantle. According to her, and the R&D staff at ACtronics she has spoken to, when the circuitry within a product is glued together with the cover itself it is hard to dismantle the circuitry and keep it intact. In most cases the circuitry is destroyed and useless. However, it is identified that even if the circuitry is destroyed information can still be derived from it, albeit more difficult. A similar protection can be used for the sensor. By using custom made glue in order to glue the circuitry to the cover a good protection can be created.

Using these types of protective measures can be argued as a measure that makes it hard for a person skilled in the art to access the sensor. This was identified as an important aspect when the trade secret was identified as 'put on the market'. This protective measures obstructs a person skilled

in the art to easily access the information within the sensor and thereby enabling the protection given from at least the FHL.

14.2 NDT

Non-destructive testing is a wide group of analysis techniques used in industry to evaluate components or systems without causing damage.[184] There are many different methods that can be used in order to analyse components or systems without causing damage, e.g. use of electromagnetic radiation (X-rays), ultrasonic testing, radiographic testing, acoustic emission etc. In order for this thesis to not be too technically complicated this thesis will only analyse how to protect the sensor from electromagnetic radiation and ultrasonic testing.

Using electromagnetic radiation, in order to analyse components, is a commonly used method and almost any material can act as an electromagnetic shield. However, a shield made of high-density material is better than low-density material.[185] Therefore, one effective way to block the radiation that does not require extensive amounts of material is to use a 'lead shield'. Lead has a very high density and is therefore often used in order to protect from electromagnetic radiation. This method is used in many sectors and the ordinary person has seen this method at the dentist. It is the collar around the neck when taking x-ray photos of the teeth. Therefore, a cover of lead is one way to protect the sensor. Lead has however many negative properties. It is expensive, heavy, and has a negative impact on the environment.[186] Another solution is to cover the sensor with steel. Steel has not as high density as lead and requires therefore greater thickness in order to be as effective. It is possible to use x-ray through steel as thick as 2.5 inches (6.35 cm) and 3.5 (8.89 cm) if using gamma ray.[187] Covering the sensor with a 6.35 to 8.89 cm cover of steel is identified as impractical. The sensor would be ponderous, unattractive, and expensive. Therefore, protection from electromagnetic radiation is a risk that might not be able to overcome without unreasonable costs. However, it is still identified that a steel cover will pose as a challenge for many traders, but if someone really wants to perform NTD with electromagnetic radiation, they might acquire the information within the sensor.

---

[184] "What is NDT?", Retrieved 22/04/2014 from http://www.ndt-ed.org/AboutNDT/aboutndt.htm.

[185] "Materials used in radiation shielding", Retrieved 11/04/24 from http://www.thomasnet.com/articles/custom-manufacturing-fabricating/radiation-shielding-materials.

[186] "Lead - PB", Retrieved 11/04/2014 from http://www.lenntech.com/periodic/elements/pb.htm#Environmental%20effects%20of%20lead.

[187] "Can you x-ray through steel", Retrieved 22/04/2014 http://wiki.answers.com/Q/Can_you_x_ray_through_steel?#slide=2.

Ultrasonic testing (henceforth referred to as UT) is a commonly used NDT method. UT uses high frequency sound energy to conduct examinations and make measurements. The risk is that a trader uses UT to derive information from the sensor since, if used correctly, it is highly accurate in determining reflector position and estimating size and shape.[188] However, there are limitations with ultrasonic testing. It is for example hard to use UT when the materials are rough, irregular in shape, very small, exceptionally thin, or not homogenous.[189] Furthermore it is hard to inspect materials that are coarse grained due to low sound transmission and high signal noise. Cast iron is for example such material. A protective measure could therefore be to include cast iron in the shell of the sensor. This will pose as a protective measure from UT but, as mentioned above, it might still be able to use other NDT methods to acquire some information. The possible protections from NDT have the issue that not only do they not offer impenetrable protection, they are also very ponderous.

Protection given by any of the measures enables a more limited and controlled circle of people as well as showing that the objective prerequisites are fulfilled, thereby enabling the protection given in block 1.

14.2.1 Camouflage

Another protective measure that could be used is to camouflage the components. By not marking the different components with essential data, such as what it is or what voltage they use, the infringing party will need to analyse each product herself in order to understand what they are. It is identified that the infringer will suspect that some components are standard, i.e. a certain circuitry, motherboard, or any other component, but the infringer cannot be sure of it. If however it is possible to make all the components "look" the same – in the sense that they all for example have the shape of squares and the same dimensions – it is identified as a further camouflage that makes it even more difficult for the infringing party.

Another way to utilise camouflage is to use components that acts like dummies. The dummies do not provide or do anything within the sensor other than confusing the infringer of what is the correct construction and use of components. This ought to be a fairly cheap protective measure that can be utilised to a relative great extent.

---

[188] "Basic principles of ultrasonic testing", Retrieved 23/04/2014 http://www.ndt-ed.org/EducationResources/CommunityCollege/Ultrasonics/Introduction/description.htm.
[189] ibid.

The first step of this solution – disguising the components by not marking them – and the use of dummies are identified as a feasible solution that most likely is relatively cheap. However, if the infringer really wants to know what components are used this solution will only hinder her for some time.

Utilising camouflage as a protective measure does not either strengthen or weaken the claim made in block 1 or 2. It might be argued that it fulfils the objective criterion as set out in the FHL but that means that it will need to be communicated towards the customer that the components have been camouflaged. If so it helps enabling the protection given by the FHL.

14.3 Transfer

Protecting the sensor from being transferred can be done in several ways. The most conventional ways are to, at least when the sensor is mounted on the machine and not built in within the bearing itself, weld, glue, or to throb the sensor onto the machine. By doing this it is harder for the trader to dismount the sensor from the machine. However, the trader can transfer the whole machine itself or break open the protecting cask. The protection given by these conventional measures is therefore relatively low. Other more sophisticated solutions can be used. Installing a GPS transmitter within the sensor is one way to keep track of where the sensor is. The GPS can for example be codified to release a signal when it is transferred outside of the factory it was supposed to be used in. The protection offered by this solution is very high since it can easily show whether or not there is an attempt to transfer the sensor. However, there are limitations with this solution as well. Using GPS might be expensive, it requires surveillance from time to time, and it might interfere with the measures conducted by the sensor.

Utilising these measures strengthens at least the protection given in block 1. These practical measures – as mentioned in section 14.1.3 – enable a more limited and more controlled circle of people, i.e. maintains the secret character of the sensor.

14.4 Stealing

Given that the sensor is located within the factory of the trader, there is a risk is that someone from inside, i.e. an employee, steals the sensor. In order to protect from this scenario the sensor should be, as mentioned before, protected by a secondary shell. A secondary shell is identified as sufficient protection since a single employee will find it challenging to open it up and steal it without being caught in the act. However, the solution is not bullet proof. If many employees collaborate they might be able to steal the sensor. The risk is although identified as low.

In order to not reiterate see section 14.1.3 and 14.3.

14.5 Bankruptcy

When a trader enters into bankruptcy it is presumed that everything within the control of the trader is owned by the trader, e.g. machines, facilities, IPRs and so on. In a situation where the trader has licensed the sensor the presumption is that she owns the sensor. In order to break this presumption the licensor, SKF, needs to show that it is the owner of the sensor. This can be done in several ways. The easiest way is ensure that the sensor has a serial number engraved and that this serial number is written down in the license agreement. With such a solution SKF can show fairly easy that they are the righteous owner of the sensor.

Notifying the serial number affects neither the claim made in block 1 or block 2. However, it is identified that it facilitates the transaction of trade secrets as it lowers this risk.

14.6 Conclusion

After analysing the referred practical solutions the conclusion is drawn that they are only obstacles that can be breached if one really wishes to do so. It is therefore not possible to set up impenetrable protective measures that ensure that no one will ever acquire the information within the sensor. The existence of companies such as "ACtronics" shows that it possible to overcome sophisticated protections. It is furthermore identified that there is a possibility to use several solutions in combination in order to improve the protection. For example, the sensor can have its circuitry glued together with the moulded cask and have a GPS transponder inside with a secondary shell consisting of cast iron to protect it. The logic is that the more practical solutions used, the better protection is offered. However, using many practical solutions might not be possible from a business perspective since the costs can be unreasonable. It is therefore important that an overall assessment is done for each case in order to invest in the solution that offers the best protection. Another conclusion that can be drawn is that the practical protection will most likely stop most traders to try to acquire the knowledge within the sensor. Many companies will refrain from this simply because they do not need the information or lack the resources to dismantle the sensor. It is the competitors that are identified as the threat. The worst-case scenario is that they develop the same sensor by reverse engineering and compete with SKFs using SKFs own technology. Another scenario is that the competitors develop the same knowledge from their own R&D investments. This is a possible scenario since the trade secret protection offers not exclusive right to the knowledge.

It is further concluded that the practical measures are closely linked to the protection given by block 1. The analysis shows that it is often time a necessity to utilise some protective measures in order to enable the protection given by the FHL or the Directive. Therefore, when utilising trade secrets dynamically there is a need to utilise practical measures.

Following Petrusson's and Heiden's theories, the act of protecting the knowledge by practical measures, can be identified as a property claim in the business arena since it is a claim that the knowledge is considered as a trade secret. By protecting the knowledge within the sensor, SKF displays towards the business arena that this knowledge is their property, their trade secret. This is closely connected to the first claim, that of claiming the knowledge as a secret according to the legal definition since the protective measures are more or less a requirement to fulfil the legal definition. The use of such protection is added to the belief that the asset, the knowledge within the sensor, can be trusted as potentially secure object in commercial transactions, i.e. allowing the knowledge to be capitalised through dynamic use of trade secrets.

The practical measures are not bound by any national boundaries, the business arena ought to be the same in each country. This implies that the practical protections are possible to utilise in all countries.

15 Block 3 - Practical Measures for Openly Available Knowledge

As has been seen, the protection granted by FHL and the Directive is not sufficient to grant a satisfactory level of protection when transferring the manual to a customer. It is however established that contractual provisions and other laws to some extent offset this issue. The question is how, and if, it would be possible to protect the manual using practical measures in such a manner that you would not need to rely solely on only laws and contracts. It will also be analysed how these practical measures affect the claim and protection of FHL and the Directive. Initially solutions that are more general to their character are reviewed and are then followed by specific solutions to the risks identified under section 7.2.1.

15.1 Time-Limited Access

When licensing the manual the customer will only have access to the manual for the duration of the licensing agreement. If the access to the manual during this time was limited to for instance only working hours, risks in relation that an employee may misappropriate the manual might be lowered. It builds on the assumption that the employee has work tasks to do during the working hours and would not have time to photograph the manual or similar. If the employee has possibility to take a

break and have access to the manual without any supervision or similar the limitation in time would not work as effectively or at all. If utilising a digital manual limiting the access time may be done by setting the properties of for instance the document or the data room where the manual is stored. For an analogue manual it would be required that someone is responsible for locking the manual into a safe or similar at a certain hour.

By limiting the access time of the manual the activity criterion of FHL and most likely the Directive will be fulfilled. If the customer somehow manages to access the manual after working hours, this might be seen as an acquisition, depending on the circumstances. Since SKF have shown that they do not want this to happen by limiting the access time, the acquisition would then be considered unwarranted.

15.2 Too Much Information

One way to minimise the amount of information within the manual would be, if possible, to attach external elements to it. If for instance a value needs to be calculated from a measured value, instead of showing the equation that should be used for calculating the second value, the initial value could be typed into an apparatus that would deliver the second value. This way vital information can be kept secret. If using an apparatus the information within can be subject to several risks itself, which are addressed under the section about embedded knowledge in this thesis. Instead of an apparatus an interactive manual or a field on a webpage or similar could be used and thereby avoid issues relating to the physical nature of the apparatus. Nonetheless, the customer could possibly reverse engineer the equation even though it might take long time.

Limiting the information in the manual using any of the measures above implies that the activity criterion according to FHL and most likely the Directive is fulfilled. Also, if the customer would access the information hidden either in the apparatus or the webpage this would without doubt be considered an acquisition according to FHL and the Directive. The customer does not have consent for doing this and should not be in good faith considering the acquisition either, since the information is hidden. This implies that the acquisition would be seen as unwarranted according to FHL and the Directive.

It should be noted that limiting the knowledge within the manual might affect the trade secret claim in block 1 and thereby the protection granted if limited too much. This would be the case if the information prerequisite of the FHL and the Directive would not be fulfilled. Most times this should not be an issue, due to the low requirements for knowledge and information to be claimed as trade secrets according to both the FHL and the Directive. If this is the case the

knowledge within the device or similar would still be considered as trade secrets and protected by FHL and the Directive.

Another way to limit the amount of information would be to enter most of the information in the manual, so that the customer can do most of the mounting of the bearing herself, but leave out essential moments that need to be performed by technicians of SKF. This way the most important information in the manual might be protected, however, the customer might not be very fond of this arrangement as she will have to rely on technicians from SKF and from a business perspective it might therefore not be feasible. This measure implies that the activity criterion in FHL and most likely the Directive is fulfilled since it effectively keeps the information secret. However, it does not affect the protection or claim granted by said legal acts.

15.3 Keeping the Manual

As is accounted for above under section 7.2.1.2 there are several different ways that the manual could be copied in order to keep the manual. However, all of these ways to copy the manual could potentially be solved by one simple, low tech, solution. Regardless of how the manual is transferred to the customer, either digital or analogue, having an SKF employee that supervise the use of the manual will make it impossible or at least very difficult to misappropriate the trade secret. However, such a solution is not very convenient and the customer may not be fond of having an SKF employee there all the time. Supervising the use of the manual implies that the activity criterion according to FHL and maybe the Directive is fulfilled. It does not affect the claim or the protection granted from said legal acts, apart from that SKF might be in a better position concerning evidence if the supervisor sees when for instance a disclosure takes place.

One way to prevent the customer from simply refusing to return the manual to SKF would be to utilise a data room which implies that the data is stored on a remote server, instead of on a local computer, and can only be accessed by certain devices, it is also possible to decide during which hours of the day, which users etc. that should have access. Accessing the data room should require password that only have a couple attempts after which the access would be blocked to ensure that only authorised personnel gets access to the manual. Such a data room could either be used on a computer or, more convenient perhaps, as an app on for example a tablet. To limit risks associated with temporary files that might be possible to access after the data room has been shut down SKF should supply the customer with a device through which it will only be possible to access the data room and do nothing else. By doing this SKF also ensures that the customer has never

legally acquired the manual according to FHL or the Directive. If the customer therefore manages to make a copy or similar of the manual, it will for certain imply an acquisition that is unwarranted.

To maximise the protection from the data room it should only be possible to view one part of the manual at one given time. When the step that is described in a certain part of the manual has been completed the technician may proceed to the next step in the manual. It should not be possible to go back in the manual to ensure effectiveness of this provision. If the customer needs to go back to a previous step, she would need to contact SKF to either be allowed to do that or, which is better from a control perspective, have SKF send one of their technicians to complete the previous step.

Utilising a data room is an effective way of fulfilling the activity criterion according to FHL and most likely the Directive. If the customer somehow manages to reach the manual inside the data room either after termination of the agreement or by going back to a previous section in the manual it would without doubt constitute an acquisition according to FHL and the Directive regardless if the manual is simply accessed or if a copy has been made. It is also established that SKF would not have consented to the acquisition, since the agreement is terminated. The acquisition would require hacking the data room why the customer cannot be considered to be in good faith either. Therefore it would be seen as an unwarranted acquisition according to FHL and the Directive.

15.3.1 Photographing

One way to prevent this from happening for a digital manual is to have as a demand for accessing the manual that the web camera of the computer or tablet is turned on. The camera would then be linked to the program that is used to access the manual that would see if the person operating the device takes up a phone or camera and holds in front of the screen and in such a case make the screen black. It is unclear if such a solution exist, it would however definitely be possible from a technical perspective to have such a solution when looking at what cameras can do when being applied in e.g. automobiles to detect when you are tired, when a pedestrian is in front of the car etc. As a camera has a limited visual scope, it would probably be possible to stand to the side so the camera cannot see you and take a photograph. This could however be prevented by applying a visual filter to the screen of the device that makes it possible to see what is on the screen only when you are directly in front of it. Such filters already exist and are mainly used on computer screens.[190]

The ideal solution to this problem would be if it would be possible to have a special background on the manual so that when taking a picture nothing could be seen. This solution exists

[190] Kensington, "Privacy Screen for Laptops Widescreen Flat Panel Monitors", retrieved 05/05/2014 from: http://www.kensington.com/us/us/v/4471/1687/privacy-screen-for-laptops-widescreen-flat-panel-monitors.

when it comes to copying using a colour photocopier trying to copy an analogue manual, however knowingly no such solution is unfortunately available for photographs of either digital or analogue manuals.[191] That solution is a safety paper with sections on it that becomes black and unreadable when copied using a colour photocopier. There is however a possibility to have a computer screen that is only white unless you utilise special glasses. The solution is based on that one of the polarising filters in the computer screen is removed and is then put into the lenses of the glasses.[192] It is possible to remove this filter from any computer screen rather easily implying that it should be possible also to buy a screen with the filter separated from the beginning. A filter solution would not prevent photographs from being taken, as it is possible to hold the glasses in front of the lens of the camera. However, if the glasses are stored in a safe unless for work hours it will at least make it more difficult for anyone to take a photograph, especially if the technicians would not have time to do it during their work hours. It is also possible to utilise a solution with watermarking the pages of the manual, either digital or analogue, to prevent photographs from being taken, however it would only tell that the manual belongs to SKF and not prevent the photograph from being taken.

Neither of the solutions above are very practical, and there is no identified solution for analogue manuals why this is a risk that is very difficult to be completely protected from.

All measures presented above imply that the activity criterion will be fulfilled according to FHL and most likely the Directive. If the manual is copied by taking a photograph, FHL and the Directive will consider it an acquisition. Using any of the solutions above will make it clear for the customer that SKF has not consented to the photographs, the customer will be in bad faith. Therefore it will be easier to prove that an acquisition is unwarranted according to FHL and the Directive.

15.3.2 Screenshot

The most convenient solution to this problem for a digital manual is by software preventing screenshots from being taken. This is for instance possible when it comes to a special version of PDFs called CopySafe PDF.[193] It is also possible to utilise a solution with watermarking as for photographs. It is most likely also possible to make an app for a tablet so it would be impossible to

[191] "CopySafe Copy-Preventable paper".
[192] "Privacy monitor hacked from an old LCD Monitor", retrieved 22/04/2014 from: http://www.instructables.com/id/Privacy-monitor-made-from-an-old-LCD-Monitor/.
[193] "CopySafe PDF", retrieved 31/03/2014 from: http://www.artistscope.net/copy-protect-pdf.htm.

take a screenshot in that app or that the print screen would not show what was actually on the screen.

A solution that would undoubtedly solve this problem would be if the device does not have any connection to the outer world in terms of internet, Bluetooth, USB or similar because if it does not then it would not be possible to transfer the screenshots taken to a third party anyway.

Utilising protective measures, as the ones mentioned, imply that the activity criterion of FHL and most likely the Directive will be fulfilled. It will also put the customer in bad faith when acquiring the manual by making a copy. This will make the acquisition unwarranted and ensure that the protection offered by FHL and the Directive is effective.

15.3.3 Printing

The most convenient solution for this problem for a digital manual is to have the manual stored in a virtual data room that does not allow for the manual to be printed or downloaded to later be printed. The same effect could also be achieved by having the manual as an app on a tablet. Another solution, if stored locally on a device, is to prevent the device from connecting to the printer either wirelessly or by wire.

If the manual inside the data room is printed, it will constitute an acquisition according to both FHL and the Directive. This acquisition is unwarranted since SKF has not consented to it. The customer cannot reasonably have been in good faith when acquiring the manual since the data room does not allow for the manual to be printed, a protection that would need to be circumvented. As have been mentioned above, utilising a data room implies that the activity criterion of FHL and most likely the Directive will be fulfilled.

15.3.4 Recording

This is a risk that from a technical perspective is impossible to prevent, as long as people has access to the manual, either digital or analogue, they will have the possibility to read the manual and also doing so out loud. The only way to protect the manual without having a guard, as has been discussed above, is to limit the amount of information in it, which might not be possible. In relation to this there should also be as many figures as possible instead of text describing the procedure, like an IKEA manual, as it is more difficult to read out what the picture says than just read the exact words of a text.

Utilising figures instead of text in the manual will most likely not affect the protection granted by FHL and the Directive, as the measure is rather vague. It will also most likely not fulfil

the activity criterion of either FHL or the Directive. Limiting the information or having a guard may nonetheless affect the legal protection, as have been accounted for above.

15.3.5 Copying

One way to prevent the manual from being copied is to only grant access to the manual to the people who need it in their work and only during those hours when they work. This would make it more difficult to copy the manual, as the people that would have access to it would have to perform other tasks during the time the manual is accessible. In order to prevent an analogue manual from being copied using a photocopier, safety paper, as have been discussed above, should be utilised.

The most convenient solution however, as discussed above, is to limit the information in the manual in some way to ensure that even if the manual is copied vital information will still be missing out. The solution discussed above under "Recording" with drawings as a preventive measure will not be as effective in this case as they could more or less easily be copied as well as long as the person can draw or when using a photocopier for an analogue manual.

As have been noted above, limiting the people who have access to the manual when working will ensure that the circle of people remains closed. This in turn leads to that the trade secret will not lose its secret character according to FHL and the Directive. Apart from this it does not affect the claim or protection granted by FHL or the Directive. The legal consequences for limiting the information of the manual have been accounted for above.

15.4 Transfer

There are two different ways that the manual may be transferred from a customer to a third party, which are individually addressed below. Before transferring a manual there is most times a need to make some sort of copy. The different ways that have been identified that this might be done are photographing, screenshot, printing, recording, and copying, which have all been mentioned above in relation to "Keeping the Manual" why reference is made to that section. Under that section was also mentioned that the majority of those risks could be significantly lowered, or erased completely, if an SKF employee would supervise the usage of the manual, the same principle applies for the risks in relation to transferring the manual as well.

15.4.1 Sending

One way to prevent the risk that the a digital manual file may be transferred from the customer to a third party is to have the manual on a device without communicative abilities, i.e. without any internet connection, Bluetooth or similar, implying that it would literally be impossible to send the

PDF file, or similar, containing the manual. The device could also be designed not to have any physical ports either, such as USB, to ensure that the file containing the manual is simply copied to an USB-memory or similar. Having neither physical ports nor communicative abilities is however not very practical and will pose difficulties when transferring the manual to the device. It would also be possible to limit the connective abilities of an electronic device via software, implying that the device might be used as usual, except that it would be impossible to send any files.

If digital manual is stored as a PDF file it is possible to have a time limit on the file, implying that after a certain period, for instance a month, the file will not be able to access. This will not prevent the most immediate problem that the file may be sent, it may however limit the damage from the manual being transferred.

Another solution would be to use a data room, as mentioned above, for accessing the manual which also would make it impossible to transfer the file to third parties either by internet, Bluetooth, USB memory or similar.

For an analogue manual sending is not a very big risk since the customer would then lose the manual, as long as the customer only got one manual. If this is the case there is a need to make a copy first, which is discussed above, or send it with a faxing machine. To prevent the manual from being faxed safety paper, as mentioned above, should be utilised that will make the copy of the manual that is faxed unreadable, which will work as long as it is a colour copy, if it is not this solution might not work.[194] Either way the manual should be locked in a safe outside working hours to lower this risk.

Utilising any of the mentioned measures will imply that the activity criterion is fulfilled according to FHL and most likely the Directive. If the manual is sent to a third party it will constitute a disclosure according to FHL and the Directive. Utilising any of the practical measures will ensure that the disclosure is considered as unwarranted. This is because the customer will have to circumvent the practical measures designed to prevent the manual from being sent, which implies that it cannot be considered that SKF have given an implicit consent to the transfer.

15.4.2 Stealing

It is difficult for SKF to protect the manual, either digital or analogue, from theft once it has been transferred to the customer. There are nonetheless some ways to limit this risk where the first would be to limit the amount of information within the manual so that even if it is stolen it does not pose a

[194] "CopySafe Copy-Preventable paper", retrieved 29/04/2014 from: http://www.isp-vft.com/Pages/Copysafe%2B.html.

big risk. Another way is to utilise data room or web access solution for a digital manual so that there locally is no manual that can be stolen. If having the manual stored locally on an electronic device there could be a requirement for the device to not be connected to the Internet that it cannot be hacked and the information stolen that way. A thief could of course steal the device, or an analogue manual, in such a case. The device should therefore be locked in a safe when not used, the same for an analogue manual, in order to limit the risk of theft to a minimum.

Preventing the manual from being stolen also has the positive effect that the activity criterion becomes fulfilled according to FHL and most likely the Directive. Apart from that the protective measures does not affect the claim or protection granted by FHL or the Directive.

15.5 Learning the Information

To prevent the technicians of the customer to learn the information in the manual is impossible. If one of the customer's technicians has access to the manual and performs the installations of the bearings she will sooner or later learn the information within the manual. It would however be possible to limit the risk that the individual technician learns the whole process. One way would be to switch technicians often so that they do not have time to learn what is in the manual, however, then the information would be distributed to a wide circle of people and it would be very costly to constantly switch personnel. Another way would be to have separate technicians for separate parts of the installation so that no one can learn the whole process, the backside would then be that each person would be very good at performing her part which later could be combined with the other peoples' knowledge to get the whole picture.

A better solution is to limit the information within the manual, as mentioned above, so that if the technicians of the customer learns what is in the manual it will still be limited so that they cannot install the bearings from their memory.

Switching technicians often or having separate technicians for separate parts of the installation will not affect either the claim or the protection granted by FHL and the Directive. The legal implications of limiting the information within the manual have been accounted for above.

15.6 Bankruptcy

In the case of bankruptcy of the customer SKF would like to retrieve the manual from the customer if the bankruptcy estate does not enter into the agreement. To be able to do that the manual must be possible to separate in the bankruptcy, implying that it has to be specifically marked or otherwise so that it would be possible to retrieve it. If a digital manual is accessed through a data room or another

web solution this would not be an issue though, since the customer only possess the manual temporarily every time it is accessed, and therefore has no permanent copy in the sense that it is not in the possession of the customer when not accessed and therefore the manual is returned already when the customer closes the manual on the computer or similar.

Marking the manual might, depending on how it is done might ensure that the customer is in bad faith when acquiring the manual. Apart from that it does not affect the claim or protection of FHL or the Directive. The legal implications of utilising a data room have been accounted for above.

15.7 Conclusion

As a general conclusion it can be said that the more and better practical protections added before dynamically utilising knowledge, in this case the manual, both digital and analogue, the easier and more controlled it becomes. It is however noticeable that apart from limiting the information, depending on how that may be done, the practical protections are possible to circumvent if one would really want to. The practical protections are mere obstacles in the way of getting access to the information. If a combination of solutions are used it will nonetheless obstruct getting hold of the information. The most important protective measures to apply is that the manual should be accessed through a time limited data room that is only possible to reach using a device supplied from SKF. On top of this the information within the manual, that is openly available for the customer, should be limited to a minimum by making the manual interactive as well as ensuring that the customer cannot go back to a previous section in the manual.

However, it should be noticed that the more protective solutions that are used, the more difficult it will be to utilise said solutions from a business perspective, the customer might not comply as it many times will make the use of the manual more difficult as well as increase the price of the manual. The appropriate level of protection must be determined in each individual case to ensure that the optimal benefit is gained from the costs incurred by protecting the information, as information is of different character, with different value and used in different situations. It should however be emphasised that it is many times easier to protect the manual when it is digital, as is seen above, why optimally a digital, and not analogue, copy of the manual should be transferred to the customer.

It has been noted in the majority of cases that applying practical measures implies that the activity criterion according to FHL and the Directive gets fulfilled. The practical provisions also have the positive implication that it becomes far more difficult for the customer to acquire the

manual in good faith. It is also easier to establish that for instance a disclosure is unwarranted since there will be no doubt about that SKF has not consented to the disclosure. The practical measures might also put the proprietor of the trade secret in a better position when trying to prove an infringement. Practical measures may also be tied to contractual provisions, making the contracts provisions more effective and easier to sanction if it is easier to prove an infringement.

It has also been noted that limiting the knowledge within the manual, as has been stated as one of the most effective practical protective measures, might affect the trade secret claim in block 1 and thereby the protection granted if limited too much. It is however established that most times this should not be an issue. Nonetheless the knowledge within the device or similar would still be considered as a trade secret.

In relation to the specific risks it should be noted that if licensing the manual, the license should explicitly forbid the customer to for instance take a photograph of the manual. By combining the protection from contractual provisions and practical measures a higher combined level of protection is reached. The practical measures many times also facilitates proving an infringement according to FHL and the Directive, or of a contractual provision.

Petrusson and Heiden state that it is possible to claim trade secrets in the business arena, which implies that you have information that you keep secret. Since the business arena may be global, because national borders do not necessarily bind it, it implies that all the practical protective solutions noted above in this section are possible to utilise regardless of country, as long as it is possible from a business perspective. Adding practical protections to information, such as in the case of the manual, is therefore a claiming process in the business arena implying a stronger property claim, as the control position over the information will be stronger. The question is if it would be possible to capitalise on the manual, with the information within, in terms of transacting the manual when utilising the practical protections stated above? To capitalise on the manual, it must be seen as a potentially secure object in a commercial transaction, will the practical protections enable this? As a general conclusion it can be said that if enough practical protective measures are applied, it will be a strong property claim and difficult enough to misappropriate the knowledge within the manual to capitalise on the manual by dynamically utilising the same while maintaining its value. In other cases the outcome might be different since what protections might be possible, both practically and from a business perspective, to apply will differ from case to case. Therefore, in many cases the practical protective measures that may be applied may not provide enough protection and control, why

additional protection in terms of contracts and law must be added to reach an appropriate level of protection.

16 Overall Assessment

The three different blocks have above been analysed separately in order to identify what sort of protection they offer and whether or not that protection is sufficient in order to capitalize on trade secrets, based on the works of Petrusson and Heiden. In order to do so there is a need for a summary, which is presented below. This final conclusion will address whether or not the three blocks combined will offer a sufficient protection and thereby make the foundation of a platform to dynamically use trade secrets. This section will furthermore address the findings that have been found in this thesis and their generalizability.

16.1 Embedded Knowledge

16.1.1 Summary

16.1.1.1 Block 1

In the first block the author analysed whether or not the sensor and the information kept within could be claimed as a trade secret according to the FHL and the Directive. The analysis showed that it is possible to do so but that the protection most likely is not sufficient for dynamical use. In order to facilitate dynamical use of the sensor the main problems with this claim is to maintain the relative secrecy, i.e. to maintain the control of the circle of people who knows about the trade secret, and to utilise protective measures. The protective measures will simplify the process of showing that the customer was in bad faith, as well as potentially make it to hard for a person skilled in the art to access the sensor easily. It is further concluded that selling the sensor will most likely ruin the secrecy character since the circle of people is not controlled or limited.

Theoretically, the first block contains a strong property claim derived from Swedish and European law. The claim is done in the business arena due to secrets lack of an administrative arena, and upheld finally in the judicial arena if needed. When the Directive is adopted, the claim will be stronger and more homogenous throughout the European Union. However, practically, the control position is identified as weak since it seems that the FHL and the Directive have focused on the scenario where the trader is keeping the trade secret internally, making this first block rather "toothless" when trying to use the trade secret dynamically. It should however be noted that both the FHL and the Directive offers remedies, however, these are, as shown in the analysis, hard to define and often times might not recoup the investments made.

16.1.1.2 Block 2

'Block 2' also meant a property claim, but derived from contractual claims as opposed from law. The analysis shows that the freedom of contract allows for constructing agreements that allow dynamical use of the sensor. An important aspect was that trade secrets could be acquired in good faith, why it is important to draft NDAs that put the customer in bad faith.

There are two main problems with 'block 2'. The first is that it can be, from a business perspective, hard agree upon contractual obligations stating how the sensor should be handled. The second problem derives from the nature of contractual obligations. Even if the contract can be formed so that the trade secret can be used dynamically, it has only a 'preventive effect'. A competitor who does not mind paying damages or penalties can neglect the contract and dismantle the sensor in order to access the knowledge within. The third block was analysed to address this problem. Block 2 also showed that there is a need to use contractual provisions in order to enable the protection given by block 1.

16.1.1.3 Block 3

The third block acts as a physical barrier, which prevents the trader from, to some extent, infringe on the trade secret. Several measures were analysed to prevent the customer to see and access the information, where moulding the sensor with plastic materials was identified as a commonly used measure. However, these practical measures can be used to a great extent and are limited by the cost in proportion to the sought protection. It is therefore possible to protect the sensor from most infringement attempts, but as mentioned, if a company really wants to access the knowledge, they most likely can. This is the main problem with 'block 3', that it offers no 'bulletproof' protection, but can be overridden if a trader really wants to and has the resources to do so. However, the analysis shows that it is important to utilise protective measures in order to enable the protection given by block 1.

16.1.2 Conclusion

The question is if these three blocks combined offer the necessary protection and property claims in order to capitalise the knowledge? First and foremost it is fairly easy to establish that the protection that is given by a combination of the blocks is better than relying, for example, on only the protection given by the FHL or the Directive. Adding the practical measures as a third protective step will most likely make it hard to access the knowledge for most companies since they lack the resources to utilise such operations. Therefore the use of the three blocks in combination will lower

the risk for infringement and thereby increasing the chance of SKF keeping the knowledge behind the sensor exclusive when dynamically utilising the secret within the sensor.

Following Petrusson's and Heiden's theories that in order to be capitalised, the asset needs to be viewed as a potentially secure object in commercial transaction. It is hard to establish where the threshold is for the asset to be viewed as secure enough. One way to investigate this is to compare the foundation of this platform to the system of patents. Assets, such as patents, are identified as secure objects since they undergo worldwide "investigation", have to pass thresholds, and gives the proprietor an exclusive right to the technology. Patents also have the benefit of not losing its exclusiveness even if the competitors know everything about the technology. It is moreover safe to draw the conclusion that the risk of the patent losing its exclusivity is lower than the risk of a trade secret losing its exclusivity, even if the foundation of this platform is utilised. A competitor may breach the law and the Directive, the contract, and the practical protection with damages and penalties as a consequence, prison in some cases, or simply gains the same knowledge by own R&D. As soon as they gain the knowledge kept within the sensor there is no way to 'take this knowledge back'. It is not possible to undo what someone has learned and therefore the exclusiveness of the knowledge is vanquished. The competitors can therefore build and sell copies of the SKFs sensor, without SKF being able to stop them. If the sensor were protected by a patent SKF these actions would be identified as infringements. Therefore it is rather safe to state that the market will most likely *not* identify the foundations of this platform as secure as the patent, making it an inferior system for transacting technology. However, there are some benefits. Although a cost analysis has not been made, utilising the foundation of the platform could pose as a cheaper alternative to patents. Furthermore, if utilised and not loosing the exclusivity, the foundation of this platform can offer time unlimited protection for the knowledge, as opposed to patents which generally give only twenty years of exclusivity.

16.1.3 The Business Perspective

It should first and foremost be stated that the sensor should not be sold. The risk of losing the exclusiveness is much higher if the sensor is sold since the buyer can for example legally reverse engineer the product, alternatively sell it to a third party. Therefore a business model utilising a licensing structure is recommended. With a licensing model it is easier to have a controlled and identifiable circle, thereby fulfilling the requirements in both the FHL and the Directive. Furthermore the licensing agreement should at least address the risks that are identified as imminent and connect breach of them to heavy penalties in order to create a preventive effect. Another

finding is that the licensee should in the early stages of the negotiations sign a NDA in order to show that the licensee was in bad faith when acquiring the sensor. The use of the protective measures analysed in the third block offers several different options. It is however identified that moulding the sensor with a combination of plastic and cast iron while also gluing the circuitry to this mould, is a rather effective protection from the sensor being dismantled or any other use of NDT-method, which are also identified as the most imminent risks. Combining these two practical measures with a secondary shell is identified as the best protection given that they are rather cheap compared to the protection they offer. If however there are resources, a GPS should be attached to the sensor and it should be encrypted so that only a certain computer can receive the information. These systems will reduce the risk of the licensee transferring the sensor to a third party, however, as mentioned, from a business perspective this might not be a sustainable solution.

An interesting finding, from a business perspective, is that the threshold for what should be deemed as a trade secret is low. Even if the sensor would consist of a very simple solution it is likely possible to claim it as a trade secret according to the legal definition of FHL and maybe the Directive. This means that a business model focusing on utilising trade secret can be used for almost any product. Given that there is a demand for such product, one can imagine the scenario where the foundations of the platform is used for a product that is cheap to produce. With the protection from the three blocks the knowledge of the components within can be made more or less exclusive, making it possible to raise the margins for the product since no one knows what is actually in them. Following the interview with Pernilla Hallberg, customer administrator at ACtronics, this business model is already used within the automotive industry. Cheap components are protected by practical measures and contractual claims while they are sold very expensively since no one knows that the products consist of cheap components. This business model could be a strategy in order to increase the margins on certain products within other industries as well, for example in the industry that SKF operates in.

16.2 Openly Available Knowledge

In order to make the final conclusion where the three blocks are connected to each other the findings under each block will be briefly summarised to serve as a basis for the conclusion.

16.2.1 Summary

16.2.1.1 Block 1

Claiming trade secrets is done in the business arena, due to a lack of administrative arena, and upheld in the judicial arena if necessary. It is in the first block established that the manual and the knowledge within is considered as trade secrets according to both FHL and the Directive, why the manual may be claimed as property. However, when dynamically utilising trade secrets, as in the case with the manual, the control position and level of protection granted by the FHL and the Directive is not sufficient, since they are designed for static use. The activity prerequisite also becomes more extensive for dynamic uses, especially for the Directive. Utilising confidentiality provisions or marking the manual, as 'Confidential' or 'Trade secret of SKF' will increase the level of protection, however the control and protection is nonetheless not sufficient for dynamic utilisation. When selling the manual the control is lost completely, even though it might still be a trade secret, why licensing is a preferable solution. However, both licensing and selling to a wide circle will imply that the manual loses its status as a trade secret. Both FHL and the Directive utilise prevention in terms of damages, which are difficult to establish the size of, to ensure obedience and retain control over the trade secret.

One of the main problems under the first block is to ensure that the customer is in bad faith about the manual being a trade secret, to be possible to be held responsible, which is done by utilising NDAs or marking the manual as 'Confidential' or 'Trade secret of SKF'. This will also fulfil the activity criterion of FHL and most likely the Directive. Another main problem is to ensure that the circle of people remains "identified and closed" when transferring the manual to the customer, which is done both by selecting few customers and ensuring that as few people as possible have access to the manual once transferred.

16.2.1.2 Block 2

In the second block is analysed the possibility to claim the knowledge within the manual as property using contracts, which is a weaker property claim compared to the one in the first block. Using contractual provisions fulfils the activity criterion of FHL and most likely the Directive and enables the protection granted by said legal acts. Regardless of the provisions in a contract the sanctions available are mainly penalties, which has a preventive function. In both first two blocks it is established that if a customer, that the manual has been transferred to, want to, she can do whatever she wants with the manual as long as she is prepared to pay the price in terms of damages and penalties, if detected at all.

The main problems under block 2 is the nature of a contracts and contractual obligations, and that it, from a business perspective, may be difficult to reach a common ground in the negotiations about the contractual provisions. The nature of a contract is that regardless of its design it will not actually hinder any of the parties to perform any actions, apart from the prevention it constitutes when considering the sanctions. This is the reason why the sanctions should be as severe as possible, which then again relates to the first problem of agreeing upon them.

16.2.1.3 Block 3

The third and final block is analysed as an attempt to address the issues with the two first blocks. Different practical protective measures can be utilised as means to prevent the manual from getting into the wrong hands. These measures imply that the activity criterion gets fulfilled, and enables the protection granted by FHL and the Directive, as well as the protection from contractual provisions. By limiting the information within the manual, if possible, transferring the manual could be done with very little risk. However, transferring knowledge 'openly', as with a manual, will always be done with some degree of risk. Limiting the amount of information within the manual might however have consequences for the claim and protection granted by block 1, however unlikely. It is also established that the control position is better for a digital manual than an analogue, since it is easier to protect a digital manual from the different identified risks.

The main problems for block three is how to limit the information within the manual and how to ensure a high enough level of protection. Both problems are highly depending on the individual case since the characteristics of the information will determine how much the information may be limited as well as which additional protections may be applied. There is also the issue of possibility from a business perspective, both in terms of costs and that both parties need to agree to the measures.

16.2.2 Conclusion

In order to dynamically transact trade secrets with a minimum of risks, as in the case of the manual, the question is not so much if each individual block in the thesis provide a strong enough property claim and control position to facilitate the transfer but rather if it is possible to build the foundations for a platform with enough protection and control for transferring trade secrets by combining the three of blocks.

The three blocks provide different aspects of the unity that is required for transferring trade secrets while still maintaining control over the knowledge and limiting risks. The first block provides the initial property claim and unwarranted actions that are sanctioned by damages. The second block

increases the effectiveness of the first block via confidentiality provisions while increasing the property claim overall via the contract. The second block also makes explicit what the parties may and may not do, what the sanctions are if these provisions are broken and general preventive measures such as a big up-front payment. The third block adds a practical level of protection implying an even stronger property claim as well as more or less effective methods of preventing misappropriation of the manual. Like the second block the third block increases the effectiveness of the first block.

Combining the three blocks will most likely imply a strong property claim combined with effective preventive measures and sanctions if any unwarranted actions are taken. On top of this practical solutions will make it more difficult to perform any such unwarranted actions either by will or by chance. It should nonetheless be noted that even if the control and protection will be high there are always risks associated with dynamic use of trade secrets as it is practically impossible to protect the trade secret from all sorts of risk as well as the fact that trade secrets does not give any exclusivity over the knowledge they comprise.

Petrusson and Heiden state that in order for an asset claimed as property to be capitalised upon there is a need for it to be seen as a potentially secure object in a commercial transaction. Will the trade secret be secure enough when utilising the foundation of the platform to sustain the value of the trade secret while at the same time using it dynamically? The answer is most likely yes, however the answer is dependent partly on the level of protection that can be attained by the practical protections and the prevention block 1 and 2, and partly on the strength of the proprietor of the trade secret in the business arena. If it is impossible to use any practical protections, or just a few, weak, ones, and the prevention granted by block 1 and 2 is low, the trade secret will in most cases not be secure enough to sustain the value of the trade secret while using it dynamically. This might however be offset by the strength in the business arena which can be leveraged into higher protection from legal, contractual and practical measures to arrive at a sufficient level of protection. The bottom line is therefore that even if there is no exclusivity over the knowledge, the protection and control granted by the three blocks combined should in many cases be enough for dynamically utilising trade secrets while maintaining the value of the knowledge, as long as the risk is not too big from a business perspective.

It should be emphasised that dynamically utilising trade secrets may be done regardless of level of protection, however, in such a case the associated risks will be significantly higher and it will

be more difficult to sustain the value of the knowledge, why it is not advisable to dynamically utilise trade secret without the protection from the basis of the platform.

Providing the manual through a data room that may only be accessed through a device supplied by SKF, as well as limiting the information by making the manual interactive and ensuring it is impossible to go back to a previous section in the manual are the key protective measures and will many times provide a sufficient level of protection for dynamically utilise trade secrets in a commercial transaction.

The case that have been used to visualise the possibilities and limitations is that of a manual as it is typically a text of some sort, maybe with illustrations to visualise, where the valuable information is openly available for anyone who has access to the manual. In order for the findings to be of any interest and have any impact they should be possible to generalise, to be possible to apply to other cases as well. As a manual is more or less a written document, and as it would seem reasonable that transferring knowledge protected as trade secrets would be done this way, for instance when transferring know-how as in the case or some other type of information, the findings in relation to this case are applicable to other similar cases when knowledge is transferred. The exception might be the practical solutions for limiting the information within the manual, as many times when transferring knowledge the goal is to present all of it.

As the way of transferring and controlling knowledge that is analysed in this thesis is, compared to patents for instance, relatively cheap, it is a cost efficient alternative that can be useful especially for start-ups or SMEs that might not have the resources to protect knowledge by, for instance, patent protection.

16.2.3 The Business Perspective

Since transferring the manual has its risks SKF should strive for utilising their own technicians for installing the bearings, as this will allow for SKF to remain in total control over the knowledge. However, many times this is not possible since the customer wants to install the bearings themselves. If the customer cannot agree to let SKF's technicians install the bearings there is a need to consider the value of the deal as such and compare it to the estimated value of the knowledge within the manual. If the deal is worth a lot compared to the knowledge within the manual, there are few business reasons that would speak for not entering into the business deal, even though there are risks associated with it, and vice versa.

If the manual is to be transferred to a customer it should neither be given nor be sold to the customer, as SKF will lose control over the knowledge. A better solution from a business

perspective is to license the manual instead, this model ensures better control over the knowledge at the same time, as the customer will get access to the knowledge needed to install the bearings. This model will also allow for SKF to license the same knowledge several times, with possibility of higher earnings compared to selling the manual.

It should be noted that even if there are several protective measures that may be applied it might not be possible to apply all of these measures, either contractual or practical. If the value of the knowledge is low, fewer protective measures should be applied, however, this is mainly in relation to practical solutions as the marginal cost for adding another provision in an agreement is low. There is also the issue that the parties need to agree on all the protective measures, the customer might think that the protective measures are too far-reaching in which case the parties need to negotiate a common ground.

Another aspect of increasing the protection is that it might increase the possibilities to receive higher payment for the manual if the information is limited enough so that the customer does not know what is hidden. It is possible to leverage the ignorance of the customer to increase the price, since the customer is not aware of the value of the knowledge. This is more difficult to do for openly available knowledge as compared to embedded knowledge.

17 Concluding Remarks

To dynamically use trade secrets as many protective measures from the foundations of the platform as possible should be utilised in order to maintain the value. If this is done, dynamically using trade secrets may be done with a sufficient level of protection to ensure that the value of the trade secret is maintained. If this is not done the value might be sustained anyway, but the risks associated with the transfer are higher. With these two cases the authors have shown that the foundation of the platform is applicable in a variety of cases where the owner or proprietor wants to dynamically use her trade secrets. However, the two cases also show vast differences depending on how the knowledge is packaged. When the knowledge is openly available, as in the manual case, the customer gets access to the knowledge whereas in the embedded case the customer has no initial access. The openly available case also visualises the inherent problems with knowledge, that it is non-excludable etc., which in this case for instance implies that it can be copied and spread to unlimited amount of people, whereas the embedded case cannot be 'copied' in the same way since it requires a product representation, which requires resources. Regardless of the differences of the cases many times the same conclusions are arrived to, e.g. both should be licensed rather than sold, both should be

transferred to a controlled number of customers, both need practical protective measures to ensure sufficient level of control etc.

Even if the thesis takes the perspective on knowledge owned by a 'big' company the authors believe that the findings are, and can be used generally. One can imagine start-ups or SMEs utilising the foundations of this platform as an alternative to patents in order to transact knowledge. The most obvious reasons for this is that patents are relatively costly while the foundations of the platform offer protection to lower costs. However, the question is if start-ups or SMEs are given sufficient protection from this foundation since – as the analysis shows throughout the thesis – power in the business arena, which start-ups and SMEs usually lack, might be necessary in order to get sufficient protection.

Sources

Books

- Adlercreutz, Axel, Gorton, Lars, Avtalsrätt 1, 13th Edition, Juristförlaget i Lund, 2011
- Bernitz, Ulf, Ramberg, Jan, Edenman, Ann-Charlotte, Festskrift till Jan Ramberg, 1st Edition, Norstedts juridik AB, 1997
- Fahlbeck, Reinhold, Lagen om skydd för företagshemligheter - En kommentar och rättsöversikter, 3rd Edition, Norstedts Juridik, 2013
- Folkesson, Enar, Företaget i Ekonomisk Kris, 7th Edition, Thomson Fakta, 2007
- Foray, Dominique, The Economics of Knowledge, 1st Edition, Massachusetts Institute of Technology 2004
- Gorton, Lars, Samuelsson, Per, Kontraktuella Viten, Studier i rättsekonomi - Festskrift till Ingemar Ståhl, 1st Edition, Studentlitteratur, 2005
- Heiden, Bowman J., Petrusson, Ulf, Assets, Property, and Capital in a Globalized Intellectual Value Chain, From Assets to Profits: Competing for IP Value & Return, 2nd Edition, John Wiley & Sons Inc, New Jersey 2009
- Helgesson, Christina. Affärshemligheter i samtid och framtid, Upplaga 1:1, Jure, Stockholm 2000
- Hettne, Jörgen, Otken Eriksson, Ida, EU-rättslig metod - teori och genomslag i svensk rättstillämpning, 2nd Edition, Norstedts Juridik, 2011
- Jonsson, Anna, Kunskapsöverföring & Knowledge Management, 1st Edition, Liber 2012
- Lev, Baruch, Intangibles: management, measurement and reporting, 1st Edition, Brookings Institution Press, Washington, D.C. 2001
- Levin, Marianne, Något om riskerna vid överlåtelse av know-how i samband med tillverkningsavtal - Festskrift till Jan Ramberg, 1st Edition, Nordstedts Juridik, 1996
- Levin, Marianne, Wolk, Sanna, Persson, Annina H., Immaterialrätt & Sakrätt, Upplaga 1, Jure, Stockholm 2002
- Petrusson, Ulf, Intellectual Property & Entrepreneurship Creating Wealth in an Intellectual Value Chain, 1st Edition, CIP Working Paper Series, Gothenburg 2004
- Ramberg, Christina, Ramberg, Jan, Allmän Avtalsrätt, 9th Edition, Norstedts Juridik 2014
- Sandgren, Claes, Rättsvetenskap för uppsatsförfattare – Ämne, material, metod och argumentation, 2nd Edition, Norstedts Juridik 2007

- Tonell, Magnus, Sekretessavtal - och det rättsliga skyddet för företagshemligheter, Upplaga 1, Jure, Stockholm 2012
- Wainikka, Christina, Att skydda innovationer: Affärer, risker och möjligheter, Upplaga 1:1 Studentlitteratur, Lund
- Wainikka, Christina, Företagshemligheter : en introduktion, Upplaga 1, Studentlitteratur, Lund 2010

Articles

- Bengtsson, Henrik, Kahn, Johan, (2005) Företagshemligheter i domstolarnas praxis - del 2, Ny Juridik 3:05 s 7-41
- Fontana et al. (2013). Reassessing patent propensity: evidence from a data-set of R&D awards 1977-2004
- Forrester Consulting, The Value of Corporate Secrets: How Compliance and Collaboration Affect Enterprise Perceptions of Risk. Study carried out on behalf of RSA and Microsoft, March 2010
- GE & Strategy One (2013), GE Global Innovation Barometer 2013, Global Research Report, 2013
- Logan, Lisa, The Emperor's New Clothes? The Way Forward: TV Format Protection under Unfair Competition Law in the United States, United Kingdom and France: Part 1, Thomson Reuters 2009
- OECD, New Sources of Growth - Knowledge-Based Capital Driving Investment and Productivity in the 21st Century, May 2012
- PWC, Information security breaches survey, Technical Report, April 2012.
- Stenberg, Susanne, Fransson, Martin, Företagshemligheter – En Värdeskapande Strategi, Juridiska Institutionen – Handelshögskolan vid Göteborgs Universitet, 2002
- Wainikka, Christina, Information som självständigt objekt, SvJT 2003 s 577
- Weber, Industrial espionage threatens German companies and jobs, DW.DE 29.6.2010.
- Winkler, Emil, Secrecy as a part of the intellectual value creation within a firm – How to use secrecy as a strategic tool in a business, University of Gothenburg – School of Business, Economics and Law, 2010

EU

- de Martinis, Lorenzo, Gaudino, Francesca, Respess, Thomas S. III, Baker McKenzie Study

on Trade Secrets and Confidential Business Information in the Internal Market, Milan 04.2013

- European Commission (July 2012a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Reinforced European Research Area Partnership for Excellenceand Growth, COM(2012) 392,17.7.2012. http://ec.europa.eu/research/era/index_en.htm
- European Commission, Commission Staff Working Document Impact Assessment Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Brussels, 28.11.2013
- European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, Brussels, 28.11.2013
- Justitiedepartementet, Faktapromemoria 2013/14:FPM42 Direktiv om företagshemligheter, 20.12.2013
- Naglic, Vesna, Papadopoulou, Danai, Sources and Scope of European Union Law, June 2013, retrieved from: http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.1.pdf

Preparatory Works

- Proposition 1987/88:155 om skydd för företagshemligheter
- SOU 1983:52 Företagshemligheter. Betänkade av utredningen om skydd för företagshemligheter
- SOU 2008:63 Förstärkt skydd för företagshemligheter

Presentation Slides

- Heiden, Bo, Defining Knowledge-Based Business - The Firm, The Market, and Competitive Advantage, CIP 2013

Websites

- ArtistScope, "CopySafe PDF", retrieved 31/03/2014 from: http://www.artistscope.net/copy-protect-pdf.htm
- eHow, "How to Clear Computer RAM Memory", retrieved 24/04/2014 from: http://www.ehow.com/how_5054182_clear-computer-ram-memory.html
- European Commission, "What are EU directives?", retrieved 03/03/2014 from: http://ec.europa.eu/eu_law/introduction/what_directive_en.htm

- Instructables, "Privacy monitor hacked from an old LCD Monitor", retrieved 22/04/2014 from: http://www.instructables.com/id/Privacy-monitor-made-from-an-old-LCD-Monitor/
- International Security Products, "CopySafe Copy-Preventable paper", retrieved 29/04/2014 from: http://www.isp-vft.com/Pages/Copysafe%2B.html
- Kensington, "Privacy Screen for Laptops Widescreen Flat Panel Monitors", retrieved 05/05/2014 from: http://www.kensington.com/us/us/v/4471/1687/privacy-screen-for-laptops-widescreen-flat-panel-monitors
- Lenntech.com, "Lead – Pb", retrieved 11/04/2014 from: http://www.lenntech.com/periodic/elements/pb.htm#Environmental%20effects%20of%20lead
- NDT Resource Center, "What is NDT?", retrieved 24/04/2014 from: http://www.ndt-ed.org/AboutNDT/aboutndt.htm
- SKF, "SKF Machine Condition Indicator – CMSS 200-25-PROMO Machine indication bundle", retrieved 02/06/2014 from: http://www.skf.com/binary/12-137467/CM5120%20EN%20MCA%20and%20MCI%20Promotion_tcm_12-137467.pdf
- Stackoverflow, "How are Engine Control Units (ECU) of high speed racing bikes coded?", retrieved 24/04/2014 from, http://stackoverflow.com/questions/23635784/how-are-engine-control-units-ecu-of-high-speed-racing-bikes-coded
- Techterms.com, "RAM", retrieved 24/04/2014 from: http://www.techterms.com/definition/ram
- Thomasnet.com, "Materials used in radiation shielding", retrievied 11/04/2014 from: http://www.thomasnet.com/articles/custom-manufacturing-fabricating/radiation-shielding-materials
- Webopedia, "RAM - Random Access Memory" retrieved 24/04/2014 from: http://www.webopedia.com/TERM/R/RAM.html
- Wiki answers, "Can you X-ray throgh steal", retrieved 24/04/2014 from: http://wiki.answers.com/Q/Can_you_x_ray_through_steel?#slide=2
- WIPO, "Sweden - The Act on Protection of Trade Secrets (1990:409)", retrieved 10/02/2014 from: http://www.wipo.int/wipolex/en/text.jsp?file_id=241716
- Youtube.com, "Ombyggnad av en Bosch ABS-enhet - ACtronics", retrieved 24/04/2014 from: https://www.youtube.com/watch?v=mCanmgjx-M0

Supreme Court

- NJA 1979 s. 483
- NJA 1995 s. 347
- NJA 1998 s. 633
- NJA 1999 s. 469
- NJA 2000 s. 538
- NJA 2010 s. 629

Court of Appeal

- Svea Court of Appeal Ö 4004-09
- Svea Court of Appeal Ö 9002-03
- Svea Court of Appeal T 1114/97
- Svea Court of Appeal T 8471/99

Labour Court

- AD 2013:24

Appendix 1 - Article 3 EU Directive

Article 3

Unlawful acquisition, use and disclosure of trade secrets

1. Member States shall ensure that trade secret holders are entitled to apply for the measures, procedures and remedies provided for in this Directive in order to prevent, or obtain redress for, the unlawful acquisition, use or disclosure of a trade secret.
2. The acquisition of a trade secret without the consent of the trade secret holder shall be considered unlawful whenever carried out intentionally or with gross negligence by:

   (a) unauthorised access to or copy of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced;
   (b) theft;
   (c) bribery;
   (d) deception;
   (e) breach or inducement to breach a confidentiality agreement or any other duty to maintain secrecy;
   (f) any other conduct which, under the circumstances, is considered contrary to honest commercial practices.
3. The use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder, intentionally or with gross negligence, by a person who is found to meet any of the following conditions:
   (a) has acquired the trade secret unlawfully;
   (b) is in breach of a confidentiality agreement or any other duty to maintain secrecy of the trade secret;
   (c) is in breach of a contractual or any other duty to limit the use of the trade secret.
4. The use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of use or disclosure, knew or should, under the circumstances, have known that the trade secret was obtained from another person who was using or disclosing the trade secret unlawfully within the meaning of the paragraph 3.
5. The conscious and deliberate production, offering or placing on the market of infringing goods, or import, export or storage of infringing goods for those purposes, shall be considered an unlawful use of a trade secret.

Division of Labour - Who is Responsible for What Section?

The table below represents which author, Denis Ilecic, Gustav Svensson, or both, is responsible for each section in the thesis.

Section	**Responsible Author**
Acknowledgements	Both
Abstract	Both
1-6	Both
7.1	Denis Ilecic
7.2	Gustav Svensson
8	Both
9	Denis Ilecic
10	Gustav Svensson
11	Both
12	Denis Ilecic
13	Gustav Svensson
14	Denis Ilecic
15	Gustav Svensson
16.1	Denis Ilecic
16.2	Gustav Svensson
17	Both

Jag, Denis Ilecic, registrerades på kursen första gången VT14. Jag har inte omregistrerats någon gång och har inte deltagit i något tidigare examiantionstillfälle.